МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ДОРЖИ БАНЗАРОВА

Д. Ш. Цырендоржиева, О. М. Манжуева

ФЕНОМЕН ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Монография

Улан-Удэ
Издательство Бурятского госуниверситета
2020

УДК 130.1
ББК 87.6
Ц 975

Утверждено к печати
редакционно-издательским советом
Бурятского госуниверситета

Рецензенты
Е. Ю. Захарова, доктор философских наук, профессор,
заведующая кафедрой философии, Забайкальский государственный университет
О. Б. Истомина, доктор философских наук, профессор,
заведующая кафедрой социально-экономических дисциплин,
Иркутский государственный университет
О. Б. Бальчиндоржиева, доктор философских наук, доцент,
Бурятский государственный университет им. Д. Банзарова

Цырендоржиева Д. Ш.
Ц 975 **Феномен информационной безопасности**: монография / Д. Ш. Цырендоржиева, О. М. Манжуева. — Улан-Удэ: Издательство Бурятского госуниверситета, 2020. — 308 с.
SBN 978-5-9793-1490-7
DOI 10.18101/978-5-9793-1490-7-2020-1-308

В монографии раскрыты основные положения теорий информационного общества с точки зрения безопасного использования информационных технологий. Систематизированы негативные эффекты, опасности, угрозы применения информационных технологий, выделены ключевые направления информационной безопасности в качестве основной составляющей национальной безопасности. Разработана система социальных мер обеспечения информационной безопасности, закладывающая социально-философские основы общенаучной теории информационной безопасности.

Предназначена для всех интересующихся философской проблематикой.

Tsyrendorzhieva D. Sh.
The phenomenon of information security: monograph / D. Sh. Tsyrendorzhieva, O. M. Manzhueva. — Ulan-Ude: Buryat State University Publishing Department, 2020. — 308 p.

The monograph reveals the main provisions of the theories of the information society from the point of view of the safe use of information technology. Systematic negative effects, the dangers, the threat of the use of information technology, highlighted the key areas of information security as a core component of national security. A system of social measures to ensure information security, laying the socio-philosophical foundations of the General scientific theory of information security.

The publication is intended for all those interested in philosophical issues.

УДК 130.1
ББК 87.6

© Д. Ш. Цырендоржиева, О. М. Манжуева, 2020
ISBN 978-5-9793-1490-7 © Бурятский госуниверситет им. Д. Банзарова, 2020

ПРЕДИСЛОВИЕ

Единое планетарное сообщество сегодня становится реальностью. В обеспечении жизнедеятельности новой цивилизации особая роль принадлежит информации и знаниям, стабильность ее функционирования определяется качеством информационно-технологических решений. В то же время данный процесс обладает амбивалентным характером: устойчивое развитие социума уже немыслимо без целенаправленной глобальной информатизации, с одной стороны, и повышением степени уязвимости социальных объектов от информационного воздействия – с другой.

Во всех сферах жизнедеятельности общества четко обозначился класс новых видов угроз и опасностей, связанных с применением новейших технологических средств, которые обладают множеством вариантов своего проявления: искажение информации, фальсификация реальности виртуальными мирами, манипулирование сознанием людей, подмена целей и образа жизни навязанными стандартами, информационные войны и т. д. Рожденное глобализацией общее информационное пространство размывает основы идентичности, ведет к потере отдельными странами своей автономности. Непрекращающийся рост мощности информационных технологий, их масштабное внедрение привели к трансформации системы ценностей, современное общество испытывает глобальный ценностный кризис. В подобных условиях совершенно очевидно, что доминанта информационной безопасности неизмеримо возрастает.

Перечисленные процессы и многие другие, прежде всего, обусловлены социальными аспектами информационного взаимодействия. Осмысление совокупности информационных процессов относительно обеспечения их безопасности обретает большое значение для общества. Сложившаяся ситуация свидетельствует о необходимости адекватной фило-

софской рефлексии, выработки новой аксиологической парадигмы, соответствующей новой формуле бытия. В этой связи вполне закономерен поиск основополагающих ценностей, которые зададут ориентиры грядущего развития общества, заложат фундамент, поддерживающий внутренний мир человека, определяющий устойчивость общества в целом. Качественно новый подход, рассматривающий информационную безопасность не только в конкретно-прикладных аспектах, а как внутреннее состояние всей социальной системы, представляется перспективным направлением в изучении проблем данной области, обеспечивающим эффективное функционирование и успешное развитие как информационной сферы, так и социума в целом.

На сегодняшний день очевидна необходимость в том, что действующая система безопасности России должна организовать защиту основных прав и свобод, гарантировать равноправное участие всех субъектов информационного взаимодействия в системе глобальной безопасности. В этой связи значение исследований социально-философского характера информационной безопасности только возрастает, поскольку она способствует реализации таких ключевых обязанностей государства, как обеспечение безопасности в информационной сфере, формированию оптимальных условий для его интеграции в глобальное информационное сообщество, выработке научно обоснованной общей теории информационной безопасности. Социально-философское исследование информационной безопасности связано с формированием качественной системы информационной безопасности, отвечающей требованиям современного общества, создающей безопасные условия для дальнейшего поступательного движения цивилизации, а также для насущных потребностей данного этапа развития Российской Федерации.

Актуальность темы исследования определяется, прежде всего, новизной самой проблемы информационной безопас-

ности, в особенности ее социально-философской составляющей, сфокусированной на обеспечении безопасности общества и человека, изучении его ценностных предпочтений на фоне трансформирующейся реальности. Указанная проблематика имеет определенную степень разработки, но в то же время исследования носят фрагментарный и несистемный характер. Изучение данной темы обладает большим значением для понимания специфики информационной безопасности и ее огромного влияния на дальнейшее развитие общества.

ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННОГО ОБЩЕСТВА

1.1. КОНЦЕПТУАЛИЗАЦИЯ ПОНЯТИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Формирование информационного общества является закономерным этапом эволюции современного социума, характеризующегося, в первую очередь, масштабным внедрением информационных технологий и развитием глобального информационного пространства. Процесс становления нового общества, обусловленный внедрением информационных технологий, нуждается в верном осознании его информационной специфики и конструктивном развитии заложенного в нем потенциала.

Проблема защиты от проявившихся в третьем тысячелетии новых видов опасностей и угроз, порожденных информатизацией, беспокоит исследователей современного общества. Количество работ, посвященных проблемам информационной безопасности, постоянно растет. В то же время, анализ научной литературы доказывает, что методологические аспекты изучения информационной безопасности требуют дальнейшей проработки. Согласно нашей точке зрения, прежде всего, важно исследовать терминологию, поскольку авторы многочисленных работ в области информационной безопасности сходятся во мнении о том, что дать исчерпывающее определение информационной безопасности чрезвычайно сложно. «Отсутствие общепринятых понятий и категорий, – пишет российский исследователь Г. А. Атаманов, – приводит к полисемии, а порой и к омонимии, что, в свою очередь, значительно снижает эффективность научных разработок в области безопасности, особенно их прикладное

значение»[1]. Попытки выработать дефиницию, ясно и точно отражающую содержание рассматриваемого феномена, предпринимаются постоянно, поскольку определение сущности информационной безопасности относится к числу проблем, решение которых обладает как теоретическим, так и практическим значением.

Каждое явление, объект или процесс обладает внутренним содержанием и соответствующим ему внешним выражением. Сочетание двух указанных составляющих позволяет получить полное представление о предмете исследования и направлениях использования его результатов.

Прежде чем приступить к исследованию понятия «информационная безопасность», сначала вполне логично определить, что представляет собой безопасность. Эпикур видел безопасность в гармонии человека и природы[2]. Л. Валла связывал ее с понятием мира и дружбы[3]. Т. Гоббс понимал безопасность в двух добродетелях: вере и законах[4]. Дж. Локк говорил, что для безопасности необходима разработка опытно-практического и теоретического знания[5]. Проблемы безопасности также нашли свое отражение в идеях русского космизма[6], в контексте глобальных проблем русские мыслители искали научные пути совершенствования мира. Эволюция общества изменяла представления о безопасности, различные философские направления посредством собственных

[1] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 106.

[2] Мыслители Греции. От мифа к логике. М. : Эксмо-пресс, Харьков: Фолио. 1998. С. 774.

[3] Валла Л. Об истинном и ложном благе. О свободе воли. М. : Наука. 1989.

[4] Гоббс Т. Левиафан. М. : Мысль. 2001. С. 396.

[5] Локк Дж. Сочинения: в 3 т. Т. 2. М. : Мысль. 1985.

[6] Вернадский В. И. Несколько слов о ноосфере // Ноосферные исследования. – 2013. Вып. 1(3); Федоров И. Ф. Философия общего дела. М. : Книга по требованию. 2012; Циолковский К. Э Промышленное освоение космоса. М. : Машиностроение, 1989; Чижевский А. Л. Космический пульс жизни: Земля в объятиях Солнца. Гелиотараксия : сб. трудов. М. : Мысль. 1995.

гносеологических оценок знание о безопасности наполняли специфическим содержанием.

Современная литература рассматривает понятие «безопасность» в качестве системы условий и факторов, в которых объект органично функционирует и развивается по своим внутренним законам[1]. Так же безопасность трактуют как состояние, при котором нет опасности, то есть «условий и факторов, угрожающих существованию индивида или сообществу»[2]. Безопасность часто определяется как способность объекта сохранять свои системообразующие свойства при деструктивных воздействиях, дезорганизующих основные параметры и характеристики, потеря которых ведет к утрате объектом своей сущности[3]. Кроме того, под данным понятием так же имеется в виду система гарантий, обеспечивающая нормальное развитие любого явления[4].

Важно заметить, что практически все перечисленные определения подвергаются критике, как со стороны ученых, так и со стороны специалистов-практиков[5]. На наш взгляд, несостоятельность многих определений проявляется в том, что при конкретизации понятия «безопасность» не учитывается ее диалектическая противоположность – опасность, это

[1] Заплатинський В. М. Терминология науки о безопасности. Zbornik prispevkov z medzinarodnej vedeckej konferencie «Bezhecnostna veda a bezpecnostne vzdelanie». – Liptovsky Mikulas: AOS v Liptovskom Mikulasi. 2006.

[2] Дзлиев М. И., Романович А. Л., Урсул А. Д. Проблемы безопасности: теоретико-методологические аспекты. М. : МГУК. 2001. С.9.

[3] Стрельцов А. А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. М. 2001. № 4.

[4] Федеральный закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности»// Российская газета. Федеральный выпуск № 5374. – 2010. 29 декабря.

[5] Дзлиев М. И., Романович А. Л., Урсул А. Д. Проблемы безопасности: теоретико-методологические аспекты. М. : МГУК, 2001; Кузнецов В. Н. Российская идеология XXI века в обеспечении эффективности и безопасности динамично-устойчивого развития России [Электронный ресурс]. URL: http://spkurdyumov.narod.ru/Kuznetsov25.htm (дата обращения: 16.02.2014).

обстоятельство не позволяет раскрыть данный термин наиболее точно и подробно. Безопасность обретает смысл в связи с проявлением опасности, как ее производная, верно пишет Г. А. Атаманов[1]. Автор указывает, что «опасность» характеризует состояние объекта, при котором наличие внутренних или внешних воздействий нарушает механизмы жизнеобеспечения системы, в результате чего возникает угроза нормальному режиму его функционирования. Он так же отмечает, что не всякая угроза дисфункции обязана восприниматься как опасность, а та – которая угрожает его функциональной целостности: «безопасность возникает как преодоление опасности»[2].

В этом ключе прав В. П. Петров, говоря о том, что «система безопасности, основанная на подходе, который не учитывает состояние опасности, утрачивает смысл, поскольку настроена не на преодоление опасности, а на оправдание существования собственно социальной системы»[3]. При этом автор констатирует, что в настоящее время не разработано теоретическое обоснование той предметной области, которая способна определять сферу безопасности. «Понимание безопасности под углом “жизненно важных интересов личности, общества и государства” содержит в себе внутреннее смысловое противоречие и является недостаточно корректным в научном отношении»[4], – заключает автор.

[1] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 106.
[2] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 108.
[3] Петров В. П. Информационная безопасность России в условиях глобализации // Политическое образование [Электронный ресурс]. URL: http://www.lawinrussia.ru (дата обращения: 15.08.2014).
[4] Петров В. П. Информационная безопасность России в условиях глобализации // Политическое образование [Электронный ресурс]. URL: http://www.lawinrussia.ru (дата обращения: 15.08.2014).

Данную точку зрения поддерживает А. В. Макеев: «Интересы, важность которых не вызывает сомнений, необходимо формулировать и реализовывать, обеспечивая те или иные потребности личности, общества и государства посредством целенаправленной социально-политической деятельности»[1]. Речь идет не о защите интересов людей как таковых, но базовых условиях существования людей, государства и общества в целом, закрепленных в системе ценностей и жизненных устоев. В результате чего сфера безопасности должна быть представлена как социальное пространство, охватывающее основы общественного бытия и базовые ценности человека.

Таким образом, можно заключить, что безопасность определяется, как возможность системы противостоять опасностям, а так же способность переходить в своем развитии к более высокому уровню. Процедура защиты безопасного состояния необходима для нормального функционирования и прогрессивного развития системы. На наш взгляд, безопасность рассматривается в качестве одной из характеристик жизнеобеспечения любого объекта, а так же в качестве имманентной способности данного объекта реагировать на искажение собственных ценностей, целей, интересов, иначе, оснований существования данной системы.

Определив понятие «безопасность», перейдем к анализу сущности понятия «информационная безопасность». На наш взгляд, информационная безопасность – это уникальный феномен современного общества, формирование которого имеет глобальное значение для всего человечества, вследствие чего жизненно необходимо сформулировать его объективное, практическое определение.

[1] Макеев А. В. Основы политики национальной безопасности: структурогенез и механизм реализации: автореф. дис. ... д-ра полит.наук. М., 1999. С. 22-23.

Сложность освещения проблемы информационной безопасности до настоящего времени, как отмечают специалисты[1], связана с отсутствием общепринятого толкования терминов, описывающих рассматриваемую предметную область. Наряду с термином «информационная безопасность» активно используется термин «безопасность информации». Не вызывает сомнений тот факт, что данные понятия взаимосвязаны. При этом очень важно внести уточнение: «безопасность» сама по себе не существует, то есть безотносительно к объекту, как верно отмечает А. А. Стрельцов, «без определения объекта понятие “безопасность” является неопределенным, оно лишается внутреннего смысла»[2]. Содержание понятия «безопасность» предопределяет выбор объекта. В таком случае, если объектом защиты выступает сама информация, понятия «безопасность информации» и «информационная безопасность» становятся синонимами. В то же время, если объектом защиты рассматривать другой какой-либо объект или субъект в качестве участника информационного взаимодействия, тогда в термине «информационная безопасность» слово «информационная» уточняет направление деятельности, соответственно, понятие «информационная безопасность» следует трактовать как состояние защищенности указанного объекта (субъекта) от угроз различного характера в информационной среде. В свою очередь, А. А. Малюк вносит четкое разграничение между терминами «информационная безопасность» и «безопасность информации», уточняя, что «безопасность информации – состояние защищенности информации от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности (уничтожения, искажения) или несанкционированного ис-

[1] Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. М. : Горячая линия-Телеком. 2001. С. 7.

[2] Стрельцов А. А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. 2001. № 4. С. 12.

пользования», а вот трактовка понятия «информационная безопасность» «определяется тем контекстом, в котором оно употребляется»[1].

Характеризуя современное состояние изучаемой проблемы, С. П. Расторгуев пишет следующее: «Ранее как никогда актуальная проблема защиты информации подобно монете перевернулась, от чего родилась защита от информации, ее прямая противоположность»»[2]. Теперь возникла необходимость в защите самой системы и, что наиболее важно, человека от информации, поскольку любая поступающая информация в систему неизбежно ее изменяет. Так, целенаправленное деструктивное информационное воздействие может привести систему к необратимым последствиям, вплоть до уничтожения.

Действительно, информационная безопасность достаточно сложный феномен, кроме того, существуют некоторые условия, создающие трудности в определении данного понятия. Выделим основные:

1. Информационная безопасность – объективный феномен, вызванный объективными условиями развития социума. Его формирование происходит на фоне процесса информатизации общества, который, в свою очередь, сам находится на стадии становления и требует дальнейшего внимательного изучения. Кроме того, особенности информационной безопасности в Российской Федерации связаны, прежде всего, с реформированием самой системы национальной безопасности страны. В результате существования перечисленных факторов возникают трудности, не позволяющие сформулировать достаточно полное определение изучаемого понятия.

[1] Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. М. : Горячая линия-Телеком. 2001. С. 7.

[2] Расторгуев С. П. Философия информационной войны. М. : Вузовская книга, 2002. С. 45.

2. Трудности в определении понятия «информационная безопасность», на наш взгляд, обусловлены еще тем фактом, что феномен информационной безопасности исследуется в различных аспектах: техническом, правовом, психологическом, социальном и т. д. Ученые, рассматривающие этот феномен с точки зрения своей научной области, наполняют понятие «информационная безопасность» собственным содержанием, тем самым еще раз подчеркивая ее многогранную природу, что налагает некоторые затруднения в процессе выработки единого определения. В результате чего исследования носят специализированный характер и рассматривают информационную безопасность с определенных научных позиций. Философский анализ, проведенный в рамках нашего исследования, должен обобщить существующие представления об информационной безопасности, в целях выработки средств и методов, повышающих эффективность решений поставленных перед ней задач. Необходимость философского осмысления информационной безопасности бесспорна, потому как только философское изучение на базе синтеза существующих исследований в состоянии вывести единое понимание феномена.

Рассмотрев основные трудности, встречающиеся исследователям на пути решения проблемы сущности информационной безопасности, перейдем к раскрытию основных подходов к определению информационной безопасности. Попытаемся в целом охарактеризовать рассматриваемые подходы к определению понятия «информационная безопасность», которые условно можно разделить на технологический и гуманитарный[1].

[1] Астахова Л. В. Информационная безопасность: герменевтический подход: монография. М. : РАН. 2010. С. 86; Иншаков М. В. Обеспечение информационной безопасности России в условиях становления глобального информационного общества: автореф. дис. … канд. полит. наук. М. 2007; Шерстюк В. П. О развитии в МГУ научных исследований и учебного процесса в области информацион-

Технологический подход к определению информационной безопасности, по мнению В. П. Шерстюка, рассматривает данное понятие с точки зрения развития индустрии информатизации, обеспечения безопасности информационно-телекоммуникационных систем, обеспечения потребностей национального рынка информационно-технологической продукцией и выходом ее на мировой рынок[1].

Так, В. Н. Ясенев считает, что «информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, в узком смысле информационная безопасность подразумевает: защиту информации от внесения в нее изменений неуполномоченными лицами; сохранность ценных данных; надежность работы компьютера; сохранение тайны переписки в электронной связи»[2]. В. А. Васенин в контексте решения проблем компьютерного терроризма представляет информационную безопасность в качестве «совокупности мер, методов, механизмов, инструментальных средств и мероприятий, позволяющих обнаружить и предотвратить путем оперативного реагирования на действия, способные привести: к несанкционированному доступу к охраняемой законом информации, носящей высокий уровень секретности, нарушению ее целостности, защищенности, конструктивной управляемости; к разрушению инфраструктуры сети посредством вывода из строя системы управления ею или отдельных ее эле-

ной безопасности // Научные и методологические проблемы информационной безопасности. М. : МЦНМО. 2004.

[1] Шерстюк В. П. О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности. М.: МЦНМО. 2004.

[2] Ясенев В. Н. Информационная безопасность в экономических системах. Н. Новгород: ННГУ. 2006. С. 8.

ментов»[1]. А. Н. Асаул утверждает, что информационная безопасность – «совокупность средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа»[2]. В данном контексте самое лаконичное определение информационной безопасности дают В. Ю. Гайкович и Д. В. Ершов: «Информационная безопасность есть обеспечение защиты от различных воздействий естественного и искусственного характера информации, а также поддерживающей инфраструктуры»[3].

Вышеприведенные определения в рамках технологического подхода ярко демонстрируют приоритетный объект защиты информационной безопасности: основное внимание сконцентрировано исключительно на проблеме защиты информации и информационной инфраструктуры. При этом под информационной инфраструктурой предполагается совокупность организационных структур, технических средств, аппаратного и программного обеспечения для хранения информации, с целью ее дальнейшей обработки и передачи. Подобный подход вполне объясним, он определяет одну из сущностных сторон информационной безопасности. С технологической точки зрения информация является «продуктом»[4] информационных технологий, соответственно, требует защиты.

На наш взгляд, подход, согласно которому информационная безопасность в качестве приоритетного объекта защиты рассматривает информацию и поддерживающую ее ин-

[1] Васенин В. А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности. М. : МЦНМО. 2004. С. 80.

[2] Асаул А. Н. Организация предпринимательской деятельности. СПб. : АНО ИПЭВ. 2009. С. 257.

[3] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий [Электронный ресурс]. URL: www.twirpx.com (дата обращения: 26.05.2010).

[4] Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. М. : Горячая линия-Телеком. 2001. С. 6.

фраструктуру, является односторонним, поскольку не определяет наличие других, не менее важных ее сторон, таких как, например, субъекты информационных отношений (личность, общество, государство) или информационная среда, под которой понимаются «совокупность информационных ресурсов (то есть различных форм организации информации о жизнедеятельности общества), системы формирования, распространения и использования информации»[1]. Более того, указанный подход не характеризует социально-психологические и социально-политические аспекты информационной безопасности. При этом важно заметить, что независимо от существующих недостатков, он остается доминирующим над остальными. «Технологическая составляющая информационной безопасности разработана более тщательно и глубоко, в то время как гуманитарная составляющая – гораздо слабее»[2], – верно отмечает В. П. Шерстюк.

Сторонники гуманитарного подхода исследования проблем данной области убеждены в том, что информационная безопасность – социальное явление, прежде всего гуманитарно-технического характера. В этом ключе М. В. Иншаков доказывает двойственный характер информации: «Поскольку информация существует объективно-физически, ее изучают физика, математика и технические науки; с другой стороны, информация существует и субъективно, в таком статусе ее должны исследовать психологические, биологические, философские и социально-гуманитарные науки. В то же время естественнонаучная (техническая) сторона информационных процессов является подчиненной частью, главное направление исследований находится в области социально-

[1] Петров В. П. Информационная безопасность России в условиях глобализации // Политическое образование [Электронный ресурс]. URL: http://www.lawinrussia.ru (дата обращения: 15.08.2014).

[2] Шерстюк В. П. О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности. М. : МЦНМО. 2004. С. 38.

политического, гуманитарного анализа»[1]. А. Е. Войскунский также отмечает междисциплинарный характер информационной безопасности, в результате чего заключает, что ее разработка должна носить комплексный характер[2].

Л. В. Астахова, доказывая генетическую гуманитарную сущность информационной безопасности, приходит к выводу: «любая деятельность в своей структуре имеет ряд компонентов: цель, объект, субъект, процессы, методы, средства и результаты. Даже самый беглый взгляд на структуру действий по обеспечению информационной безопасности позволяет рассмотреть гуманитарные особенности ее основных компонентов»[3], так, по мнению автора, «гуманитарная сущность информационной безопасности субъекта определяет и гуманитарную сторону деятельности по обеспечению информационной безопасности»[4].

Гуманитарный подход рассматривает информационную безопасность с точки зрения проблем, связанных с обеспечением духовного обновления общества, соблюдением конституционных прав и свобод граждан в области информационной деятельности. Основные вопросы указанного подхода составляют такие проблемы, как формирование методологических основ обеспечения информационной безопасности; становление информационной безопасности в качестве междисциплинарной отрасли научного знания; развитие правового регулирования; обеспечение безопасности массового, группового и индивидуального сознания; исследование места и роли информационной безопасности в социальных

[1] Иншаков М. В. Обеспечение информационной безопасности России в условиях становления глобального информационного общества: автореф. дис. … канд. полит. наук. М. 2007.

[2] Войскунский А. Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. № 1(3). С. 49.

[3] Астахова Л. В. Информационная безопасность: герменевтический подход. М. : РАН. 2010. С. 86.

[4] Там же.

процессах современного общества[1]. Так, А. Д. Урсул и Т. (Ф). Н. Цырдя, определяя информационную безопасность как срез всех видов деятельности общества, в которых индустрия информатики занимает важное место, дают следующую трактовку изучаемого понятия: «информационная безопасность – это способность государства, общества, социальной группы, личности, во-первых, обеспечить с определенной вероятностью достаточные и защищенные социальный интеллект и информационный ресурс, оптимальную социальную энтропию и инфосреду для поддержания жизнедеятельности и жизнеспособности, устойчивого функционирования и развития социума; во-вторых, противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации; в-третьих, вырабатывать личностные и групповые навыки и умения безопасного поведения; в-четвертых, поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано; в-пятых, постоянно и последовательно по определенной безопасной программе "вмонтировать" искусственный интеллект в социосреду»[2]. Несмотря на то, что формулировка понятия верно отражает специфику информационной безопасности, у нее есть существенный недостаток – данное определение в попытке охватить все сущностные стороны информационной безопасности довольно громоздкое, в результате чего сложное для восприятия.

[1] Шерстюк В. П. МГУ: научные исследования в области информационной безопасности // Информационное общество. М. : МЦНМО. 2005. Вып. 1. С. 49.

[2] Урсул А. Д., Цырдя Т. (Ф). Н. Информационная безопасность. Сущность, содержание и принципы ее обеспечения [Электронный ресурс]. URL: http://security.ase.md/publ/ru/pubru22.html (дата обращения: 22.08.2014).

В то же время в научной литературе представлены исследования[1], направленные на конкретизацию социальных, психологических, политических, правовых, педагогических и других аспектов информационной безопасности. Однако необходимо отметить, не все из перечисленных направлений предлагают концентрированное определение изучаемого понятия в рамках собственного видения проблем изучаемой области. В целях реализации поставленной перед нашим исследованием задачи рассмотрим такие наиболее выделяющиеся из гуманитарных разработок проблемы информационной безопасности, как нормативно-юридический и психологический подходы.

Нормативно-юридический подход представлен в законах и нормативных документах Российской Федерации и других зарубежных стран, регулирующих отношения по обеспечению информационной безопасности. Так, Доктрина информационной безопасности Российской Федерации в термин «информационная безопасность» вкладывает следующий смысл: информационная безопасность – это «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[2].

В Законе РФ «Об участии в международном информационном обмене» (утратил силу) информационная безопасность подразумевала состояние защищенности в информационной среде, предполагающее ее развитие в интересах

[1] Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М. : РАГС. 1998; Гришина К. В., Морозова Е. В. Вопросы социально-психологического обеспечения деятельности комплексных систем защиты информации // Безопасность информационных технологий. 1997. № 1; Ершов Д. А. Информационная безопасность личности как цель социально-педагогической деятельности [Электронный ресурс]. URL: http://scipeople.ru/group/125/topic/196 (дата обращения: 19.08.2014) и др.

[2] Доктрина информационной безопасности РФ // Рос. Газета. 2000. 28 сент.

государства, организаций и граждан[1]. Важным недостатком указанных определений, как пишут М. И. Дзлиев, А. Л. Романович и А. Д. Урсул, является их «расплывчатость»[2]. Более того, Г. А. Атаманов считает, что «некорректно в законе рассматривать в качестве объектов защиты “интересы”, “государство”, “общество” и “личность”, поскольку они не являются субъектами права. Субъектами права являются физические и юридические лица, а также исполнительные органы власти. … В данном контексте рассматриваемые понятия разносущностны, в результате чего несопоставимы и крайне расплывчаты»[3]. На наш взгляд, определения законодательных документов отличаются слишком общим содержанием рассматриваемого понятия «информационная безопасность», что говорит об их несовершенстве.

Из зарубежных стран в первую очередь необходимо отметить США как страну, обладающую самой длинной историей изучения проблем в области информационной безопасности. В Соединенных Штатах Америки первый закон о защите информации был принят в 1906 году. В настоящее время в США число законодательных актов по защите информации составляет около 500 документов. Выделим из них национальный план защиты инфраструктуры (National Infrastructure Protection Plan – NIPP), в котором Министерство внутренней безопасности США определило информационную безопасность как комплекс мероприятий, направленных на защиту компьютеров, цифровых данных и сетей их передачи от несанкционированного доступа и действий, связанных с манипулированием, кражей, порчей (искажени-

[1] Федеральный закон № 85-ФЗ от 04.07.1996 «Об участии в международном информационном обмене» // Собрание законодательства РФ. 1996. № 28. Ст. 3347.
[2] Дзлиев М. И., Романович А. Л., Урсул А. Д. Проблемы безопасности: теоретико-методологические аспекты. М. : МГУК. 2001. С. 9.
[3] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 106.

ем), блокированием, уничтожением умышленного и случайного характера [1]. Данное определение, как большинство определений информационной безопасности, обладает чертами, присутствующими во многих трактовках, в качестве объекта защиты здесь установлена, прежде всего, компьютерная информация, в виде цифровых данных и сетей их передачи.

Анализ уголовного законодательства современных государств, контуры которого мы обозначили, показывает, что понятие «информационная безопасность» в качестве общепринятого термина не отражено. Преступления в сфере информационных технологий интерпретируются в качестве преступлений в сфере оборота компьютерной информации и киберпреступления (Германия (§ 202a, § 206, § 269, § 274, § 303a, § 303b, § 317)[2], Франция (ч. 1 кн. 2 разд. 2 гл. 6 от. 5; ч. 1 кн. 4 разд. 3 гл. 2 от. 2 §4)[3]. Отсутствие в мировом сообществе единого, обоснованного в научном плане подхода к пониманию сущности информационной безопасности серьезно препятствует консолидации усилий стран мира в борьбе с проблемами использования информационных технологий.

Уголовный кодекс РФ также не дает определение информационной безопасности, преступления, совершенные в данной области расцениваются как преступления, совершенные в сфере компьютерной информации, в качестве объекта защиты выступает информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если деяние повлекло уничтожение, блокирование, модификацию или копирование

[1] Национальный план защиты инфраструктуры США. National Infrastructure Protection Plan – NIPP [Электронный ресурс]. URL: http://net.educause.edu (дата обращения: 18.08.2014).

[2] Уголовный кодекс ФРГ. М.: 1996; Уголовный кодекс Федеративной Республики Германии. Особенная часть [Электронный ресурс]. URL: http://law.edu.ru/norm/norm.asp?normID=1242733&subID=100102942,100102944#text (дата обращения: 10.02.2015).

[3] Уголовный кодекс Франции. СПб.: Юридический центр Пресс. 2002.

информации, нарушение работы ЭВМ, системы ЭВМ или их сети[1].

В Модельном уголовном кодексе, рекомендательном законодательном акте для Содружества Независимых Государств содержится раздел XII «Преступления против информационной безопасности», здесь в качестве объекта защиты рассматриваются компьютерная информация и компьютерные системы[2], при этом трактовка самого понятия «информационная безопасность» отсутствует. Наличие подобного факта в законодательных документах приводит к неоднозначности определения, тем самым вызывая осложнения в правоприменительной практике. Кроме того, юридические формулировки, в первую очередь, заняты последовательностью оценки тяжести акта, совершенного преступления.

Стоит заключить, что нормативно-юридические определения, направленные на изучение информационной безопасности с точки зрения законодательства, также отличаются односторонностью, они определяют степень виновности и меру наказания по факту осуществленного преступления по отношению к компьютерной информации и компьютерным сетям в границах государства. Кроме того, юридические определения не учитывают социальные аспекты феномена информационной безопасности.

Психологический подход расставляет акценты на психологической составляющей информационной безопасности. Последователи данного подхода, вопреки распространенному мнению, что кибернетическая природа определяет основу информационных воздействий[3], считают, что исследования

[1] Уголовный кодекс Российской Федерации. М. : Проспект, КноРус, 2010. С. 129.
[2] Модельный уголовный кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств (с изменениями на 16 ноября 2006 года) [Электронный ресурс]. URL: http://docs.cntd.ru (дата обращения: 18.08.2014).
[3] Расторгуев С. П. Информационная война. М. : Радио и связь. 1998.

информационной безопасности должны опираться на психологические данные[1].

А. Е. Войскунский, исследуя психологические аспекты информационной безопасности, определяет рассматриваемое понятие как кибербезопасность[2]. Поскольку автор не уточняет ее трактовку, приведем определение данного термина, указанного Ю. В. Бородакием, А. Ю. Добродеевым и И. В. Бутусовым: «кибербезопасность – это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства»[3]. Согласно точке зрения о том, что корни информационного противоборства имеют психологическую основу[4], здесь вполне логично найти отражение психологических характеристик информационной безопасности, но при этом толкование самого словосочетания «информационная безопасность» остается нераскрытым, поскольку указанное определение ограничивается условиями явной или скрытой информационной войны, для которой характерны элементы борьбы, понятие «противник», «оружие» и «ущерб», понимаемый как поражение.

Психологический подход кардинально отличается от всех существующих, поскольку выдвигает на передний план субъекта информационного взаимодействия человека, личность, он совершенно справедливо отмечает одну из сущностных сторон информационной безопасности, которой свойствен психологический аспект. Однако трактовки ин-

[1] Войскунский А. Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. № 1(3). С. 49.

[2] Там же.

[3] Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2013. № 1.

[4] Лайнбарджер П. Психологическая война. М. : Воениздат. 1962; Селезнев И. А. Война и идеологическая борьба. М. : Воениздат. 1974; Почепцов Г. Г. Информационно-психологическая война. М. : Синтег. 2000.

формационной безопасности, наиболее ярко отражающие точку зрения данного подхода, согласно нашему мнению, также являются ограниченными, поскольку защита психологического состояния человека на фоне воздействий информационной процессов – обязательный, имманентный, но не единственный элемент информационной безопасности.

Важно отметить, что психологический подход в последнее время получил активное развитие, в результате чего сформировалось новое направление социальной практики и научных исследований – информационно-психологическая безопасность.

В рамках социально-философского исследования Г. А. Атаманов определяет информационную безопасность как «результат преодоления условий, порождающих соответствующую опасность, и закрепляется в формах, которые позволяют социальным субъектам сохранить способности выработки релевантных объективным потребностям целей и возможности их достижения»[1]. С нашей точки зрения, данная формулировка отличается существенным недостатком, в ней позиционируется социальный субъект и присущие ему потребности, цели, возможности относительно неких форм и опасностей вне информационной среды, как результат – понятие теряет специфические особенности, характерные только для изучаемой нами области.

Л. В. Астахова дает следующее определение информационной безопасности – это состояние защищенности субъекта, выражающееся в безопасности информации субъекта и его информационно-психологической безопасности, достигаемое посредством рефлексивного определения и контролирования единства его естественного существования и разви-

[1] Атаманов Г. А. Информационная безопасность в современном Российском обществе (социально-философский аспект): автореф. дис. … канд. филос. наук. Волгоград. 2006. С. 7.

тия в ходе реализации информационных процессов (создания, передачи, представления, получения, обработки, хранения) как на содержательном, так и на представительном уровнях информации[1]. Автор стремится отразить в содержании понятия максимально необходимую, на его взгляд, совокупность информационных компонентов: объект, субъект, цель, процессы, деятельность, средства. В результате формулировка лишается такого свойства, как лаконичность, оно становится сложным для восприятия.

В свою очередь, изучая методологическую основу определения сущности понятия «информационная безопасность», А. И. Алексенцев трактует его как «состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиту субъектов от негативного информационного воздействия»[2]. Необходимо отметить важный момент, автор сам признает, что в определении не достаточно конкретности[3]. Действительно, в предложенном понятии отсутствует содержательная часть, наличие данного факта, в некоторой степени, сводит его к объяснению термина «безопасность информационных систем», что является крайне не правомерным, поскольку понятие «информационная безопасность» имеет более широкий смысл.

Подводя итог исследованию сущности понятия «информационная безопасность» в рамках гуманитарного подхода, необходимо отметить, что субъекты информационных отношений и информационная среда как сфера деятельности этих субъектов, связанная с созданием и потреблением информа-

[1] Астахова Л. В. Информационная безопасность: герменевтический подход. М. : РАН. 2010. С. 22.

[2] Алексенцев А. И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 20.

[3] Там же.

ции, выступают в данных определениях в качестве мета-объекта защиты.

Таким образом, спектр определений информационной безопасности широк, нами приведены наиболее характерные из них в соответствии с методологическими подходами авторов. Анализируя указанные определения информационной безопасности, отметим их основной недостаток: исследователи сконцентрированы на специфических аспектах феномена или наоборот недостаточно конкретны, в результате чего важные моменты смыслового наполнения потеряны. В конечном итоге возникает в определенном плане обедненная трактовка понятия, которая не отражает полного понимания исследуемого феномена. Мы убеждены, что в данной ситуации необходим философский подход, отличающийся всеобщностью, который позволит учесть недостатки и положительные стороны существующих подходов. К положительным характеристикам рассмотренных подходов необходимо отнести их внимание к различным аспектам изучаемого феномена, по своей сути перечисленные трактовки не противоречат друг другу, они лишь отражают разные грани информационной безопасности, что дает основание достаточно обстоятельно проработать актуальную проблему.

На наш взгляд, практически для всех исследователей при разработке определения общим являлось стремление внести не только терминологическую, но и методологическую ясность в смысловое значение понятия «информационная безопасность». Так, исходя из того, что сущность безопасности системы заключается в способности сохранять свою целостность и способность развиваться, реализовывая указанные способности в реальных условиях, в том числе и неблагоприятных (конфликта, риска, неопределенности и т. д.), приходим к главному методологическому выводу: система обеспечения безопасности, в нашем случае – информационная, направлена на реализацию перечисленных адаптивных спо-

собностей. Оттого информационную безопасность стоит рассматривать как безопасность объекта в информационной среде и как безопасность информационной сферы.

Для определения информационной среды предложим трактовку данного понятия В. П. Петровым. «Информационной средой (сферой) следует считать:

1) совокупность субъектов, участвующих в информационном взаимодействии;

2) технологии, обеспечивающие данное взаимодействие»[1].

Далее автор вносит уточнение: информационная сфера включает помимо совокупности субъектов и непосредственно информацию, предназначенную для использования субъектами информационного взаимодействия, инфраструктуру, обеспечивающую обработку, хранение и обмен информацией, а также отношения, сложившиеся в связи с формированием, хранением и распространением информации[2].

В итоге, основываясь на вышеизложенном анализе научных подходов, определим основное сущностное содержание понятия «информационная безопасность»:

1) обеспечение безопасности информации;

2) обеспечение безопасности субъектов информационного взаимодействия от негативного информационного воздействия;

3) удовлетворение информационной потребности субъектов информационного взаимодействия посредством обеспечения безопасного состояния информационной среды.

Так, наше исследование дополняет содержание информационной безопасности третьим признаком – удовлетворе-

[1] Петров В. П. Информационная безопасность России в условиях глобализации // Политическое образование [Электронный ресурс]. Режим доступа: URL: http://www.lawinrussia.ru/informatsionnaya-bezopasnost-rossii-v-usloviyakh-globalizatsii-ch-1 (дата обращения: 20.03.2015).

[2] Там же.

ние информационной потребности субъекта в процессе его информационного взаимодействия в контексте безопасного состояния информационной среды.

В. Мак-Дугалл отождествляет потребности в качестве первичной жизненной энергии[1]. К. Юнг определяет потребности непосредственно исходя из влечений, элементарных, первичных мотиваций, над которыми надстраивается жизненный опыт человека как опосредствующий механизм[2]. Потребность в теории Р. Вудвортса выступает как «промежуточная переменная» между организмом и стимулом, как механизм «готовности» организма по отношению к объекту[3].

Сегодня потребность в информации или информационная потребность является одним из центральных понятий в теории информационной деятельности. Однако при этом до сих пор не существует однозначного понимания содержания этого понятия. Согласно ГОСТ 7.73–96 «Поиск и распространение информации. Термины и определения», информационная потребность отражает характеристики предметной области, значения которых необходимо установить для выполнения поставленной задачи в практической деятельности[4]. «Модельный закон об информатизации, информации и защите информации» дает следующее определение: «Информационная потребность – потребность лица в информации для осуществления своей деятельности»[5]. В самом об-

[1] Flugel J. Prof. W. McDougall. 1871–1938. // Brit. J. Psychol. Gen. section. 1999. Vol. 29.

[2] Юнг К. Г. Проблемы души нашего времени. М. : Прогресс-Универс. 1993.

[3] Вудвортс Р. Contemporary schools of psychology, L. 1964. Экспериментальная психология М. : Изд-во иностранной литературы. 1950.

[4] Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации [Электронный ресурс]. URL: http://www.docload.ru/Basesdoc/6/6316/index.htm (дата обращения: 20.08.2014).

[5] Модельный закон об информатизации, информации и защите информации. (Постановление от 18 ноября 2005 года № 26-7) [Электронный ресурс]. URL: http://base.spinform.ru/show_doc.fwx?rgn=63035 (дата обращения: 20.08.2014).

щем смысле информационная потребность предполагает необходимость в информации, которая выражается в информационном запросе.

Изучая вопросы удовлетворения информационных потребностей субъектов информационного взаимодействия, Г. А. Атаманов отмечает, что в безусловном порядке должны удовлетворяться не любые информационные потребности, а те, «которые определяются необходимостью обеспечения жизнедеятельности субъекта, его адаптации к постоянно изменяющимся условиям окружающей среды» [1]. Автор в первую очередь в это число включает информацию, обеспечивающую формирование научно обоснованной адекватной картины мира. Далее – информацию, отвечающую за социализацию личности. После – все, что обеспечивает хозяйственную, производственную и другую легитимную деятельность субъекта. При этом важно отметить, что информационные потребности имеют исключительно персональный характер. Они зависят как от особенностей поставленных задач, также и от психологических, образовательных и других характеристик субъекта, принимающего решение. По мнению А. И. Алексенцева, требуемая для удовлетворения информационных потребностей информация должна быть: достаточной (относительно полной для принятия решений); достоверной и своевременной[2].

В свою очередь, удовлетворение информационной потребности сопряжено с опасностью: если обилие низкокачественной информации не будет исключено, значит, безопасность не гарантирована. Для того чтобы процесс удовлетворения информационных потребностей не оказывал деструк-

[1] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 109.

[2] Алексенцев А. И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1.

тивного воздействия, носил позитивный характер для субъекта информационного взаимодействия, информация должна отвечать основным требованиям: быть достоверной, своевременной и достаточной. Вероятность принятия правильного решения, как правило, определяется качеством информации и когнитивными способностями самого субъекта.

Развитую способность дифференцировать контент, анализировать информацию и находить верные решения при реализации поставленной задачи Г. А. Атаманов называет «мудростью» субъекта[1]. Отсутствие необходимой информации для принятия решений вынуждает субъекта информационного взаимодействия экстраполировать ситуацию посредством предыдущего опыта, принимающего во внимание структуру системы, состояние связей, поведение элементов и т. д. В данном процессе также имеет большое значение уже накопленный положительный опыт предыдущих поколений, как правило, закрепленный в мифах, сказаниях, моральных нормах и принципах, иначе, культуре социума. Так, в сущностном плане информационная безопасность – это состояние объекта (субъекта), при котором информационная среда, в которой он функционирует, позволяет сохранять возможность и способность реализовывать свои решения согласно целям, направленным на прогрессивное развитие. Подобное состояние равновесия всей системы определяется нами в качестве устойчивого.

Указанное выше значит, что информационная безопасность достигается не только за счет средств, методов и мероприятий, направленных на защиту информационной среды и защиту объекта (субъекта) от деструктивного воздействия, но и посредством развития способности у объекта (субъекта) уклоняться от деструктивного информационного воздей-

[1] Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 109.

ствия. Таким образом, задача обеспечения информационной безопасности состоит в том, чтобы создать оптимальные условия для функционирования информационной инфраструктуры, главный элемент которой, не компьютер, но человек, мог прогрессивно развиваться и действовать сообразно своим ценностям и целям. Подчеркнем указанную мысль как узловую в нашем исследовании.

В итоге ценности, отраженные в сознании социального субъекта, формируют его жизненные цели, мировоззренческие ориентиры, определяют потребности. Именно ценности задают основные критерии, отвечающие за выбор и обоснование действий социального субъекта в процессе функционирования в информационной сфере. Мы выдвигаем ценности в качестве одного из ключевых компонентов определения «информационная безопасность», что является отличительным признаком собственной трактовки понятия.

Выделенное основное системообразующее содержание информационной безопасности, согласно нашему мнению, определяет ее в качестве целостного социального феномена. Подводя итог нашим разработкам, выведем собственную дефиницию информационной безопасности. Информационная безопасность – устойчивое состояние информационной сферы, обеспечивающее свою целостность и защиту объектов при наличии неблагоприятных внутренних и внешних воздействий на основе осознания социальными субъектами своих ценностей, потребностей (жизненно важных интересов) и целей развития. Данное определение в концентрированном виде выражает сущность понятия «информационная безопасность». Аксиологический, гносеологический и онтологический аспекты раскрывают философское содержание рассматриваемого определения. Онтологический аспект информационной безопасности фиксирует ситуацию преодоления опасности, целью которой является обеспечение целостности объекта и устойчивого состояния информационной среды.

Антропологический аспект понятия выявляет обеспечение безопасности субъекта информационного взаимодействия. Аксиологическая составляющая понятия «информационная безопасность» отражает ценности и цели, определяющие информационные потребности субъекта. Основное содержание понятия «информационная безопасность» заключается в обеспечении безопасности информации, защите субъектов информационного взаимодействия от негативного воздействия, удовлетворении информационной потребности социальных субъектов посредством формирования безопасного состояния информационной среды. Действительно, информационная безопасность – сложный феномен объективного развития современного социума, направленный на содействие гармоничному развитию информационного общества. Обеспечение информационной безопасности, прежде всего, требует изучения негативных результатов процесса применения информационных технологий для общества и его субъектов, исследования причин их проявления, что в конечном итоге поможет выявить способы их преодоления, тем самым формируя безопасное состояние информационной среды.

1.2. ОСНОВНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ

Впервые анализ безопасности как социального явления был рассмотрен английским философом Т. Гоббсом, который исследовал взаимосвязь и взаимообусловленность безопасности государства и безопасности человека, общества[1]. Изучая безопасность, прежде всего как социальное явление, Т. Гоббс выявил ее социальную природу, в результате чего

[1] Гоббс Т. Сочинения: в 2 т. М. : Мысль. 1991. Т.2.

связал эффективность обеспечения безопасности с формированием в обществе норм поведения.

Потому как безопасность затрагивает все жизненно важные области деятельности социума, продолжительное время усилия по обеспечению безопасности относились исключительно к прерогативе государства: на основании принадлежащей ему власти оно выстраивало соответствующую систему безопасности. В то же время информационно-технологические системы в своем развитии приобрели социальные качества и сформировались в виде источника повышенной опасности. Теперь в них человек становится одновременно объектом и субъектом отношений, а также первопричиной их создания. Своим влиянием он вносит в информационные отношения элемент организации, упорядочения, равно как и дезорганизации их состояния. Отмеченное противоречие разрешается развитием и совершенствованием самих технологий современного общества, исключающих ошибки в информационно-технологической деятельности человека. Желаемый уровень абсолютной, гарантированной безопасности применения информационных технологий невозможен, потому как человек остается носителем угрозы.

Теория информационной безопасности сформулировала три базовых принципа современных систем защиты, внедряемых в практику:

- целостность данных – существование информации в неискаженном состоянии;

- конфиденциальность информации – определяемое субъектом свойство информации, предполагающее ограничение доступа для не располагающих полномочиями круга лиц, с целью сохранения ее в тайне;

- доступность информации – способность системы обеспечить беспрепятственный доступ к информации согласно полномочиям субъектов.

В целях обеспечения перечисленных свойств информации и системы, а также предупреждения опасностей информационного характера введены меры противодействия угрозам безопасности.

Процесс защиты информации предполагает постоянный процесс модификации и поддержания оптимальной работы системы защиты[1].

Под системой защиты информации предполагают сумму специальных служб, методов, средств, мероприятий по обеспечению защиты безопасности системы и циркулирующей в ней информации.

В литературе существует широкая классификация методов и средств по обеспечению защиты безопасности в информационных системах. Так, В. А. Семененко указывает в числе основных способов обеспечения защиты системы мероприятия организационного, правового, инженерно-технического, программно-аппаратного и криптографического характера[2]. М. А. Стюгин, ссылаясь на Доктрину информационной безопасности Российской Федерации, в качестве основных мер по обеспечению безопасности выделяет правовые, организационно-технические и экономические[3]. С. И. Макаренко среди уровней обеспечения информационной безопасности выделяет законодательный, административный, процедурный и программно-технический[4]. Далее он говорит о том, что политика безопасности административного уровня осуществляется посредством административно-организационных мер, физических и программно-

[1] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий [Электронный ресурс]. Режим доступа: URL: www.twirpx.com (дата обращения: 26.05.2010).

[2] Семененко В. А. Информационная безопасность. М. : МГИУ. 2005. С. 61.

[3] Стюгин М. А. Защита систем от исследования. Методы и модели построения защищенных систем и управления информацией в конфликте. М. : РРГУ. 2011.

[4] Макаренко С. И. Информационная безопасность. – Ставрополь: СФ МГГУ им. М. А. Шолохова. 2009.

технических средств[1]. Таким образом, на наш взгляд, в качестве основных мер противодействия угрозам безопасности можно выделить административные, законодательные, программно-технические и физические.

Подобную точку зрения поддерживают В. Ю. Гайкович и Д. В. Ершов, подразделяя все меры защиты безопасности информационных систем по способам их осуществления[2]. В то же время, в число указанных мер авторы верно включают и морально-этические методы. Представленная ими классификация мер защиты имеет следующий вид: организационные (административные), физические и технические (аппаратурные и программные), правовые (законодательные) и морально-этические. Сторонником представленной классификации является и Л. Хофман. К основным методам защиты информации наряду с правовыми, организационными и программно-техническими он причисляет морально-этические способы обеспечения безопасности компьютерной системы[3]. С нашей точки зрения, морально-этические меры противодействия в системе информационной безопасности требуют обязательного внедрения в практику защиты информации, а также должного уровня изучения, поскольку невнимательное отношение к данной группе методов является серьезным упущением при построении системы защиты политики безопасности. Морально-этические меры противодействия в определенном отношении универсальны, поскольку принципиально применимы на всех уровнях защиты от несанкцио-

[1] Там же. С. 92.

[2] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. М. : МИФИ. 1995. С. 96.

[3] Хофман Л. Дж. Современные методы защиты информации: пер. с англ. М. : Сов. Радио. 1980.

нированного доступа к автоматизированной системе и информации[1].

В итоге, мы заключаем, что в практике обеспечения информационной безопасности реализуется пять основных уровней мер защиты: 1) морально-этические; 2) законодательные; 3) административные; 4) физические; 5) технические. Рассмотрим действие основных мер обеспечения информационной безопасности (физических, административных, технических, правовых) и выделим на этом фоне особую роль морально-этических мер в процессе защиты информации.

Итак, одни из основных мер противодействия угрозам информационной безопасности – физические – представляют собой механические и электромеханические устройства и сооружения по обеспечению безопасности, необходимые для создания препятствий потенциальным нарушителям на пути к защищаемой информации в автоматизированной информационной системе. Технические средства защиты информации заключаются в аппаратном и программном обеспечении, входящем в состав автоматизированной системы. Организационные или, иначе, административные меры представляют собой меры защиты, регулирующие рабочие действия автоматизированной системы обработки информации, правила использования ресурсов, работу персонала.

Здесь стоит заметить, что административные меры защиты информации, скорее, необходимы для обеспечения эффективного поддержания каких-либо других видов средств защиты, но обеспечить необходимый уровень безопасности, основываясь исключительно на административных мерах, невозможно из-за присущего им ряда серьезных недостатков. В первую очередь если в организационной структуре низкий

[1] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. М. : МИФИ. 1995.

уровень дисциплины и правопорядка, то вести речь об эффективном функционировании данного вида мер бессмысленно, кроме того, с их применением связаны дополнительные неудобства работы с большим объемом формальной деятельности. Последний недостаток вызван «склонностью людей нарушать любые установленные дополнительные организационные правила, если их только можно нарушить»[1].

В свою очередь, физические и технические меры защиты применяют для сглаживания недостатков организационных мер методом установки барьеров на пути злоумышленника, а также с целью привести к минимуму возможные нарушения персонала и пользователей системы, неумышленно допущенные путем ошибок или по халатности. Основная характеристика физических и технических мер защиты заключается в том, что они строятся на основе аппаратных и программных средств и средств связи, формируя защиту автоматизированной системы обработки информации. Размер и сложность систем защиты на основе программных средств находится в дихотомии с развитием организации.

Технические средства, развиваемые в одном или нескольких направлениях, требующие определенного программного обеспечения, в известном смысле определяют деятельность по технической защите данной организации. Но необходимо отметить, как показала практика, возможность построить эффективную и бесперебойно функционирующую систему на основе одних технических средств защиты исключена. Эффективность функционирования системы защиты информационной безопасности зависит от суммы объективных и субъективных характеристик, одна из которых – степень качества аппаратного и программного обеспечения,

[1] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий [Электронный ресурс]. Режим доступа: URL:www.twirpx.com (дата обращения: 26.05.2010).

заложенного в ее основе. Качеством программного продукта, согласно определению в соответствии со стандартом ISO 8402:1994, является совокупность характеристик объекта, относящихся к его способности удовлетворить установленные и предполагаемые потребности.

В свое время Э. Деминг сформулировал 14 правил, максимизирующих результат повышения качества информационных технологий [1]. Внимательное изучение упомянутых правил позволило нам прийти к выводу о том, что из 14 пунктов только три имеют прямое отношение к технологическим характеристикам процесса создания информационных технологий, остальные из них в большей степени относятся к философии управления и совершенствованию социальных условий труда.

Так «американский гуру качества» Э. Деминг достаточно ясно отвечает на вопрос относительно повышения качества информационных технологий, определяя основные направления концентрации усилий с целью максимизирования результата. Техническая сторона вопроса заключается в повороте к процессоориентированному подходу обеспечения качества, обязывающего проводить контроль качества и исправления ошибок на каждом этапе разработки программных средств. В данном процессе большое внимание уделено созданию особой психологической атмосферы внутри предприятия: отказ от рейтинговой системы оценок, введение системы «обратной связи», устранение барьеров, мешающих людям гордиться результатами своей работы, а также поддержание в них уверенности в завтрашнем дне. Ставка в погоне за качеством информационного продукта сделана на повышение уровня образования, постоянного обучения и самосовершенствования персонала. В его теории специалисты, не

[1] Миллер Г. У. Качественная программа: будущее информационной технологии. М. : ИНИОН РАН. 1993. С. 68.

приемлющие новшеств, и неквалифицированный персонал организации являются объектами особого внимания, с недостатками профессионализма которых идет процесс постоянной борьбы. Таким образом, согласно теории Э. Деминга, качество информационных технологий прямым образом зависит от человека: от уровня образования и морально-психологических характеристик специалиста.

В данном ключе прав Г. Миллер, утверждающий, что «будущее информационной технологии зависит, прежде всего, от способности профессионалов создавать высококачественное программное обеспечение»[1]. В подтверждение данного высказывания В. А. Благодатских верно отмечает, что важное отличие программного обеспечения от других промышленных продуктов заключается в сильном влиянии человеческого фактора на производство программного продукта, так как производство программного продукта – интеллектуальная и творческая деятельность[2].

В свою очередь, Л. Константин пишет: «Тема человеческого фактора в программировании необъятна, начиная от организационной культуры и организации проектов, хаоса и дисциплины в кодировании, инструментов и методов программирования, заканчивая пользователями и пользовательскими интерфейсами. Эта широкая область охватывает особый промежуточный мир, в котором сливаются границы между техническими и социальными вопросами. Здесь психология встречается с кибернетикой, а теория и практика смешиваются друг с другом»[3]. Основным тезисом его исследования является убеждение в том, что хорошее программи-

[1] Миллер Г. У. Качественная программа: будущее информационной технологии. М. : ИНИОН РАН. 1993. С. 71.

[2] Благодатских В. А. Стандартизация разработки программных средств. М. : Финансы и статистика. 2006. С. 188.

[3] Константин Л. Человеческий фактор в программировании. М. : Символ-Плюс. 2004. С. 3.

рование берет начало не в высоких технологиях и инструментах, хорошее программное обеспечение создается людьми, как и плохое. Согласно его убеждению, основным предметом внимания в вопросах технических мер защиты информации и систем является не аппаратное (hardware) и не программное (software) обеспечение, а человеческий фактор в программировании (peopleware). Анализируя процесс роста мощности технологических решений, автор приходит к выводу, что на пути создания и применения информационных технологий «мы встретили врага – это мы сами. Мы являемся проблемой, и мы же являемся ее решением»[1].

Таким образом, качество технической защиты, образующей каркас системы безопасности, зависит, прежде всего, от профессиональных и личностных характеристик рабочего: ошибки и недостатки, как в компьютерных программах, так и в аппаратных средствах – неизбежный спутник информационной технологии, повышение качества – это никогда не прекращающийся процесс. Изложенное выше говорит о необходимости постоянной работы с персоналом организации в целях повышения образовательного уровня, формирования благоприятной психологической атмосферы в коллективе и воспитания определенных морально-этических установок. Гипотеза о создании абсолютно надежных технических и физических средств защиты, отсекающих всякую вероятность существования открытого канала утечки информации, всегда оставляет возможность воздействия на сотрудников организации, обеспечивающих бесперебойное функционирование системы. Слаженную эффективную работу этих специалистов по обеспечению корректной работы технологических средств защиты В. Ю. Гайкович и

[1] Константин Л. Человеческий фактор в программировании. М. : Символ-Плюс. 2004. С. 13.

Д. В. Ершов справедливо называют «ядром безопасности» всей системы[1].

Анализируя статистику возможных сбоев и нарушений системы безопасности, мы видим, что, согласно данным Национального института стандартов и технологий (NIST), только 10 % случаев приходится на преднамеренные попытки получения несанкционированного доступа через внешние источники, 4 % всех возможных нарушений занимают вирусы, 15 % относятся к проблемам физической безопасности. Наиболее распространенными источниками нарушений безопасности являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационную систему, на их долю приходится 55 % случаев, к 16 % относятся действия обиженных и нечестных сотрудников организации. Уволенные сотрудники, знакомые с порядками в организации, как оказалось, способны весьма эффективно навредить. Виновными в кражах и подлогах, в большинстве расследованных случаев, оказывались штатные сотрудники организации, отлично знакомые с режимом работы и защитными мерами[2].

В результате защита информации во многом зависит от личных качеств работников, их способностей, формирования осознанного понимания соблюдения режима конфиденциальности. Согласно данным статистики, наименьшее количество утечек информации происходит в Японии, прежде всего подобную ситуацию связывают с системой «пожизненного найма» и развитием чувства патернализма и преданности, когда сотрудники организации причисляют себя к членам единой семьи.

[1] Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий [Электронный ресурс]. Режим доступа: URL:www.twirpx.com (дата обращения: 26.05.2010).

[2] Галицкий А. В. Защита информации в сети: анализ технологий и синтез решений. М. : ДМК Пресс. 2004. С. 77.

Так, приведенные доводы указывают на основные направления работы администрации и персонала организации по направлению усилий с целью снижения угроз безопасности. Примеры наиболее распространенных источников нарушений безопасности еще раз доказывают особую роль принятия правовых и морально-этических мер защиты информации в процессе построения системы информационной безопасности.

Правовые меры защиты предоставляют собой действующие национальные законы и нормативные акты, определяющие основные правила действий в информационной среде, ответственность за их правонарушения, тем самым препятствующие противозаконному применению информационных технологий и обеспечивающие сдерживающие условия с целью предотвращения девиантного поведения.

Морально-этические меры защиты информации складываются из традиционно сложившихся в стране или в обществе норм поведения, правил обращения с информацией. Чаще указанные нормы носят скорее рекомендательный характер, нежели обязательный в отличие от законодательно утвержденных указов, в то же время их игнорирование должно рождать осуждение в обществе, падение престижа и авторитета организации или человека. Морально-этические нормы существуют, как правило, в виде общепризнанных канонов человеческого поведения (патриотизм, честность и т. п.), также в виде принятого устава, свода предписаний или кодекса, иначе оформленных правил.

Морально-этические меры задают правила обращения с информацией и накладывают определенную степень ответственности за их несоблюдение. Различают два направления: создание и поддержание в обществе негативного отношения к нарушениям и нарушителям по отношению к информационной безопасности, в том числе и карательного характера. Второе заключается в координации действий, направленных

на повышение уровня образованности и информированности общества в области информационной безопасности. Необходимо заметить, что морально-этические и правовые меры противодействия в некотором смысле являются универсальными мерами на всех этапах построения системы защиты. В одних случаях они являются единственным способом защиты информации от неправомерных действий: злоупотребления служебным положением при работе с информацией, защита открытой информации от незаконного тиражирования и т. д. В других случаях люди просто не совершают противоправных действий не потому, что это технически сложно или невозможно, а потому, что подобные действия выходят за рамки допустимых норм в обществе, они осуждаются и, более того, наказываются.

Юридическая ответственность за правонарушения в информационной сфере, на первый взгляд, кажется одним из эффективнейших способов регулирования общественных отношений. Но реальность такова, что на правовом уровне вопросы гражданско-правовой ответственности за нарушения информационной безопасности не находят своего отражения, развитие законодательства в данной области весьма отстает от темпов роста технологий и числа преступлений в информационной среде[1]. Кроме того, сложившаяся ситуация в области применения информационных технологий требует согласования нормативно-правовой базы государства с международной практикой. Для России это касается, прежде всего, разработки стандартов и сертификационных нормативов согласно международному уровню, как в области информационной безопасности, так и в области информационных технологий в целом. Первая причина, почему необходимо прилагать усилия в данном направлении, – это высокая потреб-

[1] Евдокимов К. Н. К вопросу о причинах компьютерной преступности в России // Известия ИГЭА. 2010. № 6.

ность в защищенном взаимодействии с зарубежными партнерами, вторая – приоритетное преобладание на рынке информационных технологий аппаратно-программных средств зарубежного производства.

Следующая причина касается координации характера направления разработки и применения законодательных мер. Такая новая область деятельности, как информационная безопасность, требует применения мер скорее не карательного характера, а, в первую очередь, с нашей точки зрения, разъяснительного: в подобной ситуации важно научить, оказать помощь, чем запретить и наказать. Сегодня общество должно ясно осознать всю важность проблемы, увидеть и понять возможные пути решения поставленных задач. В этой связи необходимо скоординировать усилия научного, учебного и производственного плана. От государства в частности и общества в целом, прежде всего, требуются интеллектуальные вложения, направленные на формирование морально-этических установок функционирования в информационной среде.

Таким образом, принципиально невозможно построить абсолютно (идеально) надежную систему защиты информационной безопасности. Кроме того, систему защиты безопасности невозможно построить, основываясь исключительно на физических и технических (аппаратных и программных) средствах. В первую очередь, прочность системы безопасности определяется стойкостью и профессионализмом персонала, а повышение ее уровня происходит за счет кадровых, законодательных и морально-этических мер.

При этом важно отметить, что самые совершенные законы и эффективнейшая кадровая политика не являются достаточными для конечного решения проблем защиты. Поскольку всякий человек, даже обладающий абсолютной надежностью, не застрахован от неумышленного случайного нарушения. Кроме того, достаточно сложно воспитать такого уровня

персонал, в отношении которого невозможно предпринять различные усилия, вынуждающие обойти предписания. В данной ситуации острую актуальность приобретают морально-этические меры, являющиеся первым и последним рубежом в построении системы защиты информационной безопасности. Морально-этические принципы и ответственность каждого, основанные на принятых правилах поведения, более того, подкрепленные мерами законодательного характера, выступают решающим фактором регулирования деятельности человека в процессе обеспечения информационной безопасности.

Подобный подход, основанный на приоритете морально-этических мер в процессе обеспечения информационной безопасности, на наш взгляд, позволит найти новые направления повышения эффективности системы защиты. В данном ключе успех процесса обеспечения информационной безопасности общества зависит от защиты и сохранения нравственных, этических, интеллектуальных и эстетических основ социальной жизни. В этой связи формирование новой составляющей культуры – информационной культуры общества – теперь по праву рассматривают как один из путей решения проблем обеспечения информационной безопасности.

Технократическое восприятие действительности не способно гарантировать обеспечение безопасного состояния для общества, гармонии в социальной сфере, культуре и т. д., более того, его разрушительное воздействие способствует утрате человеком социальных ориентиров и психологических свойств. Неконтролируемое развитие информационно-технологической среды может привести человека к интеллектуальной, социальной и психологической зависимости, меняет его поведение и деформирует ценности. В биосоциальной природе психики человека заложены внутренние ис-

точники угроз информационной безопасности[1]. Личностные характеристики индивида определяют степень восприимчивости человека к информационным воздействиям, способность к критическому анализу и возможность оценки окружающей его информации. Помимо описанных способностей, характерных для каждого индивидуума, имеют место присущие каждому общие закономерности функционирования человеческой психики, которые в конечном итоге влияют на степень подверженности информационному воздействию. По убеждению В. Г. Грачева, в настоящее время знание собственных индивидуально-психологических особенностей и изучение общих закономерностей функционирования человеческой психики, реакции на восприятие малоосознаваемых воздействий становится обязательным элементом культуры человека в межличностных коммуникациях и важным условием безопасности в социальном взаимодействии[2].

В свою очередь, А. В. Тонконогов выделяет следующие направления обеспечения информационной безопасности человека[3]:

- формирование факторов, способствующих сохранению культурного наследия, развития творческого потенциала нации, организации обороны от внешних и внутренних угроз нравственных аспектов жизни каждого отдельного человека и социума в целом посредством конструктивного развития общей культуры населения, традиционных культур и искусства;

[1] Quoted in Noble D. Forces of Production: A Social History of Industrial Automation. N. Y. : Knopf. 1984. P. 72.

[2] Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты [Электронный ресурс]. Режим доступа: URL: http://bookap.info/psywar/grachev (дата обращения: 14.04.2012).

[3] Тонконогов А. В. Информационно-психологическая безопасность в системе духовной безопасности современной России // Власть. 2010. № 6. С. 56.

- формирование факторов, способствующих развитию и защите от внешних и внутренних угроз интеллектуальных аспектов жизни социума посредством конструктивного развития образования, науки и системы массовой информации.

На наш взгляд, сегодня информационную культуру можно определить в качестве одного из главных факторов элиминации отрицательных эффектов использования информационных технологий, гуманистической направляющей указанного процесса. Информационная культура общества предполагает наличие способности использовать информационные технологии, формировать информационные ресурсы в интересах развития и жизнедеятельности общества[1]. В то же время информационную культуру человека нельзя воспринимать только как набор приемов работы с информацией посредством компьютерных технологий. В истинном смысле ее составляют элементы, связанные с культурой информационных потребностей, этикой, саморазвитием личности, культурой компилировать знания и транслировать обществу решения познавательной деятельности. В теории информационной культуры А. М. Прихожан выделил практические навыки ее составляющие:

- развитая потребность в получении новой значимой информации;

- система взглядов, убеждений, знаний и умений, обеспечивающих правильный, целенаправленный самостоятельный поиск необходимой информации;

- умение выделять необходимую информацию для решения проблем, достижения цели;

- умение использовать различные источники информации, как традиционные, так и электронные средства информации;

[1] Ракитов А. И. Новый подход к взаимосвязи истории, информации и культуры: пример России // Вопросы философии. 1994. № 4. С. 57.

- умение анализировать информацию, отличать подлинную от ложной;

- умение критически относиться к источнику информации;

- умение сравнивать, соотносить, обобщать информацию, полученную из различных источников[1].

С нашей точки зрения, перечисленные умения составляют следующие качества и характеристики, которыми должна обладать современная личность: развитые интеллектуальные способности, критическое мышление и инновационность. Указанные особенности личности говорят об умении эффективно использовать не только информационные технологии, но и информацию, получаемую в процессе их применения, поскольку осмысление и ее выбор обусловлены только человеком. Рассмотрим, почему сегодня актуальны представленные выше качества.

Процессы образования, воспитания на переломном этапе социального развития при переходе к информационному обществу должны учитывать все нюансы изменяющейся среды, они должны соединять принцип в рамках преемственности классической культуры к новым технологическим и цивилизационным условиям развития. Здесь уже необходимо не стихийное, а сознательное, стратегическое решение вопроса, поскольку информатизация общества является объективной исторической необходимостью[2]. При этом, как было уже сказано, одной информационной технологии в качестве решающего фактора недостаточно для коренных изменений в обществе. В переходный этап важно реализовать сознательную, целенаправленную, имеющую огромное нравственное и воспитательное значение государственную политику, использо-

[1] Прихожан А. М. Информационная безопасность и развитие информационной культуры личности // Мир психологии. 2010. № 3. С. 138.

[2] Мантатов В. В., Мантатова Л. В. Этика устойчивого развития в информационную эпоху. Улан-Удэ: Бурятское книжное изд-во. 2002.

вать достижения мировой культуры для рационального переустройства своей жизни, а также руководствоваться разумным самоконтролем, опирающимся на образование и самообразование.

Так мы пришли к выводу, что защитой от деструктивного воздействия, особенно информационного, выступают ценностные установки, нравственные критерии и свойства интеллекта, то есть механизмом защиты в сложившейся ситуации выступает интеллектуализация общества. Несмотря на тот факт, что в целях решения проблем защиты от низкокачественной и негативной информации, а также чрезмерного ее потока сегодня применяются специально созданные технические средства, как поисковые средства или агрегаторы информационных ресурсов и различные когнитивные стратегии обращения к информации. При этом необходимо подчеркнуть то, что по настоящему освободить человека, сталкивающегося с потоками информации и обращений, подобные стратегии могут лишь тогда, когда он способен адекватно взглянуть на весь представленный контент. В этом ключе верно предположение Д. Фрау-Майгс: самое лучшее средство в борьбе с лавинообразным информационным потоком, самая лучшая «поисковая служба» – это образование[1]. Решая проблемы информационного характера и свободы взаимодействия пользователей, важно помнить, что человек должен быть готов воспринимать и осмысливать знаки, так как доступ к информации и автономность познающего субъекта подчиняются, прежде всего, когнитивным требованиям.

Так же в качестве одной из ведущей целей современного образования выделяют развитие критического мышления, которое выражается в способности человека к самостоятель-

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный цент научного сотрудничества. 2009. С. 58.

ному аргументированному критическому суждению о медиатекстах, иначе – умению анализировать и выявлять манипулятивные технологии современных средств массовой информации, рекламы и политических движений.

Наиболее подробно и точно термин «критическое мышление» объясняет А. В. Федотов как саморегулирующееся суждение, завершающееся анализом, интерпретацией, интерактивностью и оценкой. Критическое мышление человека в идеале связано с хорошей осведомленностью, любознательностью, причиной доверия, гибкостью, непредубежденностью, справедливостью в оценке, благоразумием в суждениях, честностью в столкновении с личными предубеждениями, желанием прояснять проблемы и сложные вопросы, пересматривать, разумностью в выборе критериев, тщательностью в поиске нужной информации, постоянностью в поиске точных результатов[1]. На наш взгляд, необходимость столь полезного качества у аудитории вызвана потребностью в осмыслении информации, передаваемой сегодня посредством коммуникационным каналов, которая зачастую бывает односторонней или искаженной.

Подобной точки зрения придерживается Л. Мастерман. Он выдвигает свою «репрезентационную» теорию, основанную на развитии у обучающихся критического мышления, что в итоге необходимо для всех граждан демократического общества[2]. В данном ключе важно выделить, что ориентация на формирование критической мысли, содействующей развитию толерантного, свободного гражданина демократического общества, владеющего автономным мышлением,

[1] Федотов А. В. Базовые теории медиаобразования // Общественные трансформации и киберпространство: междисциплинарные исследования. СПб : Факультет филологии и искусств СПбГУ. 2009. С. 108.

[2] Мастерман Л. Обучение языку средств массовой информации // Специалист. – 1993. № 4. С. 22–23.

нашла поддержку у многих ученых и общественных деятелей современности[1].

В свою очередь, А. С. Панарин на пути определения основных характеристик социально консолидированного субъекта, реализующего свою деятельность в современном обществе, особо выделяет такой регулятивный принцип, как субъектность. Принцип субъектности предполагает в первую очередь наличие воли[2]. Желание избавиться от негативного информационного воздействия должно сопровождаться возможностью проявления силы реализовать это желание, в этом заключается социальная активность индивида. В результате чего мы заключаем следующее: социально-субъективная оценка информации приобретает решающее значение и служит определенного рода призмой в потоке циркулирующей информации сегодняшнего дня.

Такая адекватная реакция на изменения среды, как воспитание критического мышления, способность ориентироваться в потоке информации, окружающей сегодня человека, являются важными составляющими его инновационности, еще одной характеристики, формирование которой, по нашему мнению, становится жизненно важным процессом для индивида и соответственно общества в целом.

Как правило, термин «инновация» употреблялся для обозначения определенных мероприятий, акций, действий в сфере техники, технологии или организации экономической деятельности[3]. Кроме этого, инновации отнюдь не ограничиваются научной, технической или технологической сферой.

[1] Gonnet J. Modes et permanences // Revue Educations. 1997. № 14; Ferguson R. Moyen de communication de mass, education et democratie // Revue Educations. 1997. № 14 и др.

[2] Панарин А. С. Стратегическая нестабильность в XXI веке. М. : Алгоритм. 2004. С. 157.

[3] Дрюккер П. Рынок: как выйти в лидеры, практика и принципы. М. : Бук Чамбер Интерн. 1992.

В данном понимании инновации не только сводятся к сфере технической или, шире, технологической деятельности, но могут касаться всех сторон общественной и духовной жизни. В этом смысле построение информационного общества представляет собой большой инновационный цикл, объединяющий в себе целый ряд глубоких взаимосвязанных и взаимообусловливающих инновационных процессов[1]. В инновационном цикле относительно синхронно происходят взаимосвязанные фундаментальные социальные инновации, охватывающие все сферы общества: от государства и общественного сознания, культуры и социальной психологии на одном полюсе до технологии и типов экономического поведения на другом. Эти циклы охватывают экономику, технику, технологию, культуру, политику, социальное поведение, государственное устройство и мировоззрение в целом.

В настоящих условиях информатизации всех процессов, протекающих в обществе, начинают действовать факторы, ведущие к изменению социального, политического, бытового поведения людей. Это не может не сопровождаться глубинными изменениями в самом менталитете. Словами Б. Метлер-Мейбом, инновационность – это «способность человека правильно вести себя в новых ситуациях»[2]. Данную способность еще называют «информационной компетентностью» или «информационной грамотностью» и считают важнейшей составляющей информационной культуры. Здесь предполагается следующее: человек должен уметь вести себя в критических ситуациях и находить верные решения для сохранения независимого и объективного мышления.

В этом смысле в определении понятия «инновационность», на наш взгляд, четко улавливается нечто общее с по-

[1] Ракитов А. И. Новый подход к взаимосвязи истории, информации и культуры: пример России // Вопросы философии. 1994. № 9.

[2] Mettler-Meibom B. Soziale Kosten in der Informatinonsgesellschaft: Uberlegungen zu einer Kommunilationsokologie. Frankfurt a.M.: Fischer Taschenbuch Verl. 1987. P. 49.

нятием «интеллигенция», т. е. свойственная человеку духовная, разумная способность постигать, схватывать, быстро находить выход, решение в необычных обстоятельствах, правильно и быстро определять главное в процессе, гибкость ума, приспособляемость, способность к быстрому мышлению[i]. Оттого именно на эту прослойку общества, более мобильную, многообещающую и менее инстинктивную, возлагаются определенные задачи. Потому как данные способности приобретают особую актуальность в процессе перехода на новый исторический этап общественного развития, поскольку он (переход) выдвигает требования реформировать социально-политическую систему, а также существенно модернизировать духовно-культурную сферу деятельности, интеллектуальный потенциал общества, радикально реформировать систему образования, воспитания и непрерывной переквалификации.

В итоге общественная практика сегодняшнего дня обязывает индивида повышать уровень своих знаний и умений, от которых прямым образом зависит его способность потреблять, перерабатывать, передавать, хранить и производить информацию. В современных условиях формирование информационной культуры приобретает жизненно важное значение для общества и каждого человека. Сегодня информационная культура задает качество человеческой деятельности, отражает уровень развития познавательных способностей и творческих сил человека, проявляющихся в методах освоения мира и организации жизни.

Таким образом, в практике обеспечения информационной безопасности реализуется пять основных мер защиты:

1) морально-этические;
2) законодательные;
3) административные;
4) физические;
5) технические.

Еще раз подчеркнем, что систему защиты безопасности невозможно построить, основываясь исключительно на административных, физических и технических (аппаратных и программных) средствах. Качество технической защиты, образующей каркас системы безопасности, зависит, прежде всего, от профессиональных и личностных характеристик индивида. Прочность системы безопасности определяется стойкостью и профессионализмом коллектива, а повышение ее уровня происходит за счет законодательных и морально-этических мер. При этом самые совершенные законы и эффективнейшая кадровая политика не являются достаточными для конечного решения проблем защиты.

В процессе обеспечения информационной безопасности как социального явления в качестве главного фактора построения системы защиты информации и регулятора деятельности человека в информационной среде выступают морально-этические принципы и ответственность каждого, основанные на принятых правилах поведения в обществе и подкрепленные мерами законодательного характера на государственном уровне. Кроме того, можно констатировать, что на сегодняшний день существует острая необходимость в целенаправленном формировании информационной культуры общества, от которой во многом зависит успешное решение проблем и вызовов, возникающих в процессе становления планетарного информационного пространства, и, соответственно, проблем информационной безопасности в целом.

В итоге основание информационной безопасности составляет деятельность социального субъекта, ясно осознающего ответственность за все свои действия. Так возникает практическая необходимость в совершенствовании и утверждении заново осмысленной системы ценностей относительно применения информационной технологии. Общественное сознание должно прочно связать понятие «информационные технологии» с понятием «нравственности», поскольку про-

цесс применения технологии в обществе должен сопровождаться разумным самоконтролем, опирающимся на нормы этики. В стремлении сохранить общечеловеческие ценности и общественные идеалы в трансформирующейся под воздействием информационных технологий социально-культурной среде возникает информационная этика как новый вид прикладной этики современного гражданского общества.

ГЛАВА 2. ИНФОРМАЦИОННАЯ ЭТИКА — ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. ОСОБЕННОСТИ, ИСТОКИ И ЭТАПЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ ЭТИКИ

Глобальное использование новых информационных технологий во всех сферах общественной жизни выдвинуло на первый план проблему роли нравственных ценностей. Человеку дана свобода творить свое будущее или лишать себя такового, предложена абсолютная нравственная точка отсчета, с которой люди всегда могут соизмерять свое творчество относительно этого будущего. Как показало время, процесс внедрения выдающихся достижений технического прогресса, протекающий без сопровождения соответствующего развития культуры в обществе, приводит к катастрофическим последствиям для человека.

Сила и мудрость – две переменные величины настоящего, между ними московский психолог А. П. Назаретян установил зависимость: чем мощнее технологии, тем более качественные средства сдерживания необходимы для сохранения социальной системы. «Суть проблемы в том, – пишет А. П. Назаретян, – что общество живет стабильно, пока разрушительный потенциал производственных и боевых технологий уравновешен качеством культурно-психологических средств сдерживания»[1]. Потеря нравственных ценностей, антигуманистический характер политико-идеологических интересов, нивелирующих мораль в современном обществе, являются одними из факторов, вызвавших кризис не только в нашей стране. Данная ситуация еще раз подтверждает мысль

[1] Назаретян А. П. Агрессия, мораль и кризисы в развитии мировой культуры. М.: Наследие. 1996. С. 60.

о необходимости формирования нового мировоззрения, поднимающего моральные ценности над технологическими, политическими и экономическими интересами.

Способность человека адекватно реагировать на изменяющиеся условия во многом зависит от сформированной аксиологии. Здесь приоритет приобретают задачи, изучающие ценности, которые в дальнейшем будут определять человеческую деятельность, направляя общий ход развития цивилизации. Какова будет общая картина системы ценностей, как разместятся в ней утилитарные и гедонистические устремления, истины жизни и познания? В конечном итоге именно система ценностей определяет человеческие стремления и задает основные ориентиры его жизнедеятельности. Э. Тоффлер, говоря о значении ценностей, предполагал, что то, какое будущее человечество себе выберет, будет зависеть от ценностей, которые определят процесс принятия им решений. А это будет зависеть от того, насколько точно человечество сумеет предсказать изменения в «целостной архитектонике ценностей», которые регулируют человеческое поведение.

При некоторых различиях общим для всех типов этических теорий является понимание морали как чего-то объективно-всеобщего, авторитетного для всех, сравнивая с чем, можно оценивать все другие ценности, нравственные позиции и проступки человека. Российские исследователи морали – С. Ф. Анисимов, Л. М. Архангельский, А. А. Гусейнов, О. Г. Дробницкий, А. И. Титаренко[1]– определяют ее как способ практически-духовного освоения действительности, а

[1] Анисимов С. Ф. Духовные ценности: производство и потребление. М. : Мысль. 1988; Архангельский Л. М. Ценностные ориентации и нравственное развитие личности. М. : Педагогика, 1987; Гусейнов А. А. Золотое правило нравственности. М. : Молодая гвардия. 1988; Дробницкий О. Г. Моральная философия: Избранные труды / сост. Р. Г. Апресян. М. : Гардарики. 2002; Титаренко А. И. Антиидеи. Опыт социально-этического анализа. М. : Политиздат. 1984.

также как способ регулирования общественных отношений и поведения человека. То есть все действия человека, включая процесс создания и использования информационных технологий, и результаты этих действий доступны оценке в понятиях этики и морали.

В стремлении сохранить духовные, нравственные, общечеловеческие ценности и общественные идеалы в становящемся глобальном коммуникационном пространстве возникает информационная этика. Формирование информационной этики как прикладной науки – это сложное динамическое поле исследований, охватывающее ценности, политику, различные концепции в контексте бурного роста технологий современного общества. В этой связи весьма важным является вопрос, раскрывающий истоки и предпосылки возникновения новой этики современного общества, а также идеи основных концепций, повлиявших на формирование принципов и характер информационной этики.

Этические проблемы развития информационно-компьютерных технологий не стоят в стороне от социальной философии. Они решаются при помощи тех же аналитических приемов и этических категорий, которые со времен античности применяются в традиционных философско-этических учениях. Философы, закладывавшие основы информационной этики, единодушны во мнении, что этико-философские истоки новой области научного знания информационного общества восходят к этике добродетели Аристотеля, философии И. Канта и утилитаризму[1]. Например, Л. Флориди новую этику в рамках своей информационной этической теории определяет как этику, берущую начало от

[1] Капурро Р. Информационная этика // Информационное общество. 2010. Вып. 5; Bynum T. The Development of Computer Ethics as a Philosophical Field of Study // The Australian Journal of Professional and Applied Ethics. 1999. № 1(1). P. 1-29; Floridi L. Information Ethics: Its Nature and Scope // Computers and Society. 2006. №36(3).

утилитаризма и этики добродетели, поскольку она нацелена для применения во всех этических ситуациях[1]. Р. Капурро рассуждает о западных истоках информационной этики, отражающих основные идеи кантианства[2]. Т. Байнам пишет, что методы, заложенные в традиционных западных теориях, таких как утилитаризм, кантианство или добродетельная этика, применяемы к рассмотрению этических ситуаций, вызванных использованием компьютеров и сетей вычислительных машин[3]. Указанная точка зрения авторов теории информационной этики, на наш взгляд, весьма точно передает основные принципы и представления о моральных нормах поведения, заложенных в систему современного этического анализа. Раскроем подробнее суть влияния наследия этики добродетели Аристотеля, деонтологической концепции И. Канта и этики утилитаризма в качестве этико-философских истоков формирования информационной этики.

Как пишет А. А. Гусейнов, философия не просто теоретическая наука, она имеет свою практическую сторону, которая выражается в этике. Этика – это та точка, в которой сливается практика с философией. Именно на данном этапе этические программы воплощаются в практике жизни, становятся полезны и необходимы людям. Это учение о том, как нужно жить и какие совершать поступки. В свою очередь, поступок здесь идентифицируется в качестве основополагающей единицы существования, этического, ответственного существования. Целевой смысл и общепринятая норма, представленные в поступке, исторически складывались в

[1] Floridi L. Information Ethics: Its Nature and Scope // Computers and Society. 2006. № 36(3).
[2] Капурро Р. Информационная этика // Информационное общество. 2010. Вып. 5.
[3] Bynum T. The Development of Computer Ethics as a Philosophical Field of Study // The Australian Journal of Professional and Applied Ethics. 1999. № 1(1). P. 1–29.

разновидности этических направлений[1]. Например, учение о добродетелях практической философии Аристотеля представляет этику в период античности. Понимание правил, подчиняющих себе поступки, в Новое время проходит через призму Кантовской практической философии, в рамках своей практической философии «диктует» поступки утилитаризм. Так, в истории человеческой цивилизации практическая философия, в образе прикладной этики, развивалась под воздействием этико-философских учений. Мы поддерживаем существующую точку зрения, что современная теория информационной этики формировалась под влиянием этики добродетели Аристотеля, деонтологической концепции И. Канта и этики утилитаризма[2]. Именно эти историко-философские учения формируют основные базисные взгляды информационной этики. Сегодня наследие их принципов и представлений о моральном поведении, заложенное в систему постулатов этического анализа, позволяет наиболее эффективно оценить модели и методы взаимодействия субъектов информационных отношений.

Практическая философия, как рассматривал этику Аристотель, убеждает, что всякая деятельность человека направлена на достижение одной цели[3]. Высшее благо – конечная истинная цель, оно является блаженством или счастьем, которое решающим образом зависит от деятельности, а именно: от деятельности души, иначе – добродетели. Так, Аристотель связывает деятельность человека со счастьем и добродетелью. «Быть достойным человеком – значит обладать

[1] Гусейнов А. А. Размышление о прикладной этике // Ведомости НИИ прикладной этики. Тюмень: НИИПЭ. 2004. Вып. 25. С. 155.

[2] Капурро Р. Информационная этика // Информационное общество. 2010. Вып. 5; Bynum T. The Development of Computer Ethics as a Philosophical Field of Study // The Australian Journal of Professional and Applied Ethics. 1999. № 1(1). P. 1-29; Floridi L. Information Ethics: Its Nature and Scope // Computers and Society. 2006. № 36(3).

[3] Аристотель. Никомахова этика. М. : Мысль. 1984. С. 54.

добродетелями»[1]. Природа добродетели, согласно его теории, заключается в разумной деятельности человека, в соотношении чувств и разума, желаний и целей. То есть все инстинктивные проявления человека – страсти и эмоции – в нравственном отношении, по сути, нейтральны, но, будучи опосредованы сознанием, получают свою ценностную ориентацию, выраженную в его действиях. Этические добродетели Аристотеля, в отличие от дианоэтических, которые воплощают добродетели высшего разума и повелевающего начала, являются приобретенными духовными навыками и формируются в процессе накопления опыта человеком. Здесь им выделены десять добродетелей, среди которых благоразумие, мужество, дружелюбие и т. д. Все они воплощают золотую середину между избытком и недостатком, например, мужество является серединой между отвагой и трусостью, щедрость – между расточительностью и скупостью, умеренность – между несдержанностью и хладнокровием. Так, в век информационных технологий заложенная Аристотелем идея добродетели приобретает особую актуальность, когда здравый смысл и рассудительность порой забыты на фоне заманчивых возможностей.

Кроме того, согласно его концепции, задача этики – направить человека и тем самым помочь ему реализоваться. Поскольку в его представлении государство являло собой более высокую инстанцию, чем отдельно взятый человек, нравственная реализация личности осуществлялась лишь через общественную деятельность. Подобная постановка проблемы Аристотелем предполагала путь социальной гармонии интересов личности и государства: ориентировала на общественное благо первого и обязывала к участию в процветании жизни своих граждан второго. Такое ценное направление для современного общества в целях достижения источ-

[1] Аристотель. Большая этика. М. : Мысль. 1984. С. 296.

ника нравственности, духовного баланса внутри себя и гармонии в обществе предлагает этика добродетели.

Утилитаризм рассматривает счастье как личную свободу, которую гарантировало основанное на принципах разума и справедливости государственно-правовое управление. Дж. Бентам предполагал, что общее благо, создающее фундамент основ морали, это есть счастье большего числа людей[1]. Данное общее благо было им названо общей пользой, исключающей какую-либо личную выгоду и корысть. Заложенное Дж. Бентамом в нормы морали принципиальное значение этой формулы блага получило дальнейшее развитие в концепции Дж. Миля[2]. В рамках теории которого анализ конкретного поступка, содеянного в личных интересах, определяется относительно направления достижения общего счастья. Таким образом, утилитаризм – теория морали, рассуждающая о правильности действия с позиции оказания добра для большего количества людей. В результате положения утилитаризма применимы для формирования критериев оценки поведения с точки зрения моральности. Приложение его принципов позволяет дать объяснение морально допустимого поступка или, напротив, аморального поведения. Применяя утилитаристский подход, мы рассматриваем полезность действий и оцениваем их последствия. Насколько моральны поступки членов информационного взаимодействия, несут ли они добро для информационного сообщества, то есть содействуют его процветанию и счастью. В противном случае общество решает вопрос о необходимости применения социальных санкций. Дж. Миль раскрывает понятие справедливости через понятие права, действуя от противно-

[1] Бентам Дж. Введение в основания нравственности и законодательства. М. : Росспэн. 1998.
[2] Милль Д. С. Утилитаризм. СПб: И. П. Перевозин. 1900.

го. Несправедливо лишать человека того, что принадлежит ему по праву закона: посягать на его физическое состояние, свободу, собственность и т. д.[1] Требование «Не навреди», являясь первичным в определении справедливости, так или иначе, встречается практически во всех правилах этических кодексов информационного общества.

В рамках деонтологической теории этики поднимается вопрос о нравственных требованиях к человеку и его действиям через призму представлений о должном и понятии долга. Самая общая формулировка описывает долг в качестве суммы обязанностей, представленных обществом личности. Главная характеристика долга проявляется в осмыслении индивидом своей ответственности перед обществом и другими людьми, в понимании моральной необходимости выполнения требований и личной стойкости. Этика И. Канта представляет наиболее известную деонтологическую теорию. И. Кант описывает моральный долг как нравственное требование для всех, как волевое состояние разумного человека. Моральная норма в конкретной ситуации становится долгом, когда преображается в личную задачу свободного индивида, осознающего свою нравственную деятельность[2]. В жизни социума это осознание приобретает особое значение, поскольку утрата чувства долга вызывает деградацию, как духовной жизни отдельной личности, так и общества в целом.

В отличие от утилитаристов сторонники деонтологической теории не ищут нравственности действий в их последствиях, они учат, что поступок человека обязан воплощать закон нравственности. Подобное философское определение долга направляет общество и индивида на воплощение моральных ценностей в практике и не позволяет поступиться

[1] Милль Д. С. Утилитаризм. СПб: И. П. Перевозин. 1900. С. 168-169, 175-176.

[2] Кант И. Сочинения. В 6 т. Т. 4. М. : Мысль. 1965. Ч. 2. С. 9, 329.

ими из-за эгоистических желаний. Согласно данному убеждению, мораль в обществе олицетворяет исполнение долга, то есть проявление ответственности и соблюдение моральных установок. Здесь правила совершения поступков И. Кант подразделяет на максимы и императивы. Максима представляет собой правило, субъективно определенное человеком, она моральна, если отвечает нравственному закону. Императив – объективный принцип, заданный разумом, который повелевает либо гипотетически, либо категорически. Гипотетические императивы условны, они оценивают поступки в каких-либо отношениях или целях. Категорический императив – предписание, объективное и идеальное во всех смыслах, это есть нравственный императив, моральный закон.

Одна из формул категорического императива И. Канта несет такой смысл: «Поступай так, чтобы максима твоей воли могла бы быть всеобщим законом»[1]. В данном случае императив призывает совершать те действия по отношению к другим людям, как желал бы человек, чтобы поступали с ним, и не совершать действий, которые не хотел бы видеть по отношению к себе. Это своеобразная форма самоустановленного человеком всеобщего закона. Следующая формула императива запрещает рассматривать человека как способ достижения собственных целей[2]. Варианты манипулирования другими людьми в качестве средства достижения личных планов ярко проявляются в цифровом мире, например, мошенничество с персональными данными, нарушение конфиденциальности информации и многие другие преступления в информационной среде. По нашему мнению, категорический императив олицетворяет всеохватывающий закон нравственности, равно как и особый всеобщий закон, принятый разум-

[1] Кант И. Сочинения. В 6 т. М. : Мысль. 1965. Т. 4. Ч. 1. С. 347.
[2] Там же. С. 270.

ным человеком, а его формулы необходимы для более доступного понимания смысла нравственного действия.

По предположению И. Канта, категорический императив способен создать в обществе новый этический строй. Как утверждает его теория, человек живет в мире регламентов и мире морали, при этом истинную свободу ему может обеспечить лишь искреннее добровольное выполнение в процессе жизнедеятельности нравственных законов категорического императива. Так, абсолютизм кантовской этики утверждает моральное право на поступок при условии его полной нравственной справедливости. Несмотря на некоторую сложность применения указанного подхода к ситуациям информационного мира, данный факт нисколько не умаляет глубокого значения теории И. Канта для этики.

Относительно основных этапов формирования информационной этики необходимо отметить, что в научной литературе, западной и российской, исследования по данной теме не встречаются. Что касается истории возникновения информационной этики, некоторые ученые предлагают искать корни информационной этики в теории и практике библиотековедения[1]. Основной тезис указанной идеи гласит: сформировавшиеся на базе информационных услуг библиотечного дела нити информационной этики плотно сплелись с концепцией компьютерной этики. Впоследствии этические вопросы, связанные с информацией на всех этапах ее жизненного цикла, стали предметом активного обсуждения в научных кругах, библиотеках, государственных учреждениях на различных уровнях и в средствах массовой информации. Поскольку концептуальное основание информационных процессов выходит далеко за рамки определения информацион-

[1] Froehlich T. Ethical considerations of information professionals // Annual Review of Information Science and Technology. 1992. № 27; Carbo T., Smith M. M. Global information ethics: Intercultural perspectives on past and future research // Journal of the American Society for Information Science and Technology. 2008. Vol. 59. № 7.

но-библиотечной услуги, мы вынуждены не согласиться с приведенным выше мнением.

Сторонники теории компьютерной этики, в свою очередь, выдвигают собственную теорию, базирующуюся на уникальной специфике этических проблем, порожденных компьютерной технологией. Прав Т. Байнам, отмечающий исключительную роль предвидения Н. Винера, описавшего будущее развитие технологий и этических вопросов, вызванных указанным феноменом[1]. Взяв идею Т. Байнама в качестве основы теории формирования прикладной этической науки, расширим ее, включив в границы изучения масштабы возможностей информационных технологий. В результате чего мы выделяем три этапа, обладающие особым значением в истории развития информационной этики.

С нашей точки зрения, первый этап развития новой информационной этики связан с именем Н. Винера, который в середине 40-х годов XX века предсказал новые этические проблемы, грядущие вслед за внедрением электронных компьютеров. Второй этап начинается с обоснования в 1976 году теории компьютерной этики в качестве отдельной дисциплины, изучающей этические проблемы в сфере использования компьютерной технологии. Третий этап сводится к появлению непосредственно самого термина «информационная этика» в 1988 году, в период зарождения глобальной коммуникационной сети Интернет. Рассмотрим более подробно каждый из выделенных нами этапов становления информационной этики в рамках философских исследований ее основателей с целью отразить вклад авторов в формирование основных идей и наиболее точно передать важные особенности новой прикладной области.

[1] Bynum T. Norbert Wiener's Vision: the Impact of the ‘Automatic Age’ on our Moral Lives, in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives. – Albany, N.Y. : SUNY Press. 2005.

На заре эпохи информационных технологий, Н. Винер предсказывает огромные социальные и этические последствия, которые придут за развитием и внедрением электронных компьютеров, и какое значение на этом фоне будет иметь этика. Он пишет, что мир подвергнется «новой индустриальной революции» – «автоматизированному веку» с «огромными потенциалами добра и зла», который произведет ошеломляющее количество новых этических проблем и возможностей[1]. Так, ученый, идентифицируя некоторые социальные и этические последствия использования электронных компьютеров, приходит к теории новой ветви прикладной этики. Он определяет круг решаемых ею вопросов: компьютеры и безопасность, компьютеры и безработица, ответственность компьютерных профессионалов, компьютеры для инвалидов, компьютеры и религия, информационная сеть и глобализация, виртуальные сообщества, дистанционное управление, синтез машин и человеческого организма, этические вопросы создания роботов, искусственный интеллект и другие темы. Предвиденные этические и социальные проблемы современного общества, связанные с созданием и использованием информационных компьютерных технологий по сей день являются объектом актуальных научных исследований в области философии, социологии, техники и т. д.

Н. Винер убежден, что общество, обладающее неограниченными возможностями на основе использования информационных технологий, должно принять «великие принципы справедливости»[2]: принцип свободы или справедливости, обеспечивающий свободу каждому человеку для развития его возможностей; принцип равенства; принцип благожелательности, пропагандирующий доброжелательность между

[1] Винер Н. Кибернетика или управление и связь в животном и машине. М. : Советское радио. 1958.

[2] Wiener N. The Human Use of Human Beings: Cybernetics and Society. Boston: Houghton Mifflin. 1954. P. 105.

людьми; принцип минимального нарушения свободы, гласящий, что любое принуждение, исходящее от общества и государства, должно осуществляться таким образом, чтобы не нарушать свободу[1]. Принятие и понимание основных принципов Н. Винера о хорошем обществе и природе человека предполагает, что существующее разнообразие культур в мире – различие обычаев, языков, религий, ценностей и практик – может обеспечить контекст, в котором люди будут иметь возможность процветать. На наш взгляд, эти принципы являются своего рода межкультурным основанием для формирующейся этики современного общества, содержащем в себе огромное культурное разнообразие. В свою очередь автор искренне верил, что их реализация возможна при значительной свободе, равенстве и превалирующей сострадательности человека.

Основываясь на практике, что в любом обществе существует сеть принятых законов, правил и принципов, регулирующих поведение человека, которые составляют «общепризнанный свод правил»[2], методология Н. Винера состоит в том, чтобы синтезировать этот общепризнанный свод правил общества с великими принципами справедливости. В справедливом обществе данные «стратегии»[3] могут служить в качестве хорошего начала для решения любого информационного этического вопроса. Мы поддерживаем убеждение автора в том, что в справедливом обществе, то есть в обще-

[1] Bynum T. Ethical Challenges to Citizens of the Automatic Age: Norbert Wiener on the Information Society // Journal of Information, Communication and Ethics in Society. 2004. № 2(2); Bynum T. Norbert Wiener's Vision: the Impact of the 'Automatic Age' on our Moral Lives, in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives. Albany, N.Y. : SUNY Press, 2005; Bynum T. Flourishing Ethics // Ethics and Information Technology. 2006. № 8(4).

[2] Bynum T., Schubert P. How to do Computer Ethics - A Case Study: The Electronic Mall Bodensee, in J. van den Hoven (ed.), Computer Ethics-Philosophical Enquiry. – Rotterdam: Erasmus University Press. 1997.

[3] Moor J. What Is Computer Ethics? // Metaphilosophy. 1985. № 16(4).

стве, где «общепризнанный свод правил» достаточно справедлив, предложенный метод анализа и разрешения информационных этических вопросов приведет к верным решениям, которые могут быть ассимилированы в общество. Кратко сформулируем и передадим основные идеи этой технологии:

1. Выделяя этические вопросы, возникающие в процессе интеграции информационной технологии в общество, необходимо фокусировать внимание на последствиях, которые оказывают влияние в первую очередь на жизнь, здоровье, безопасность, счастье, свободу, знание, возможности или на другие значимые ценности человека.

2. Грамотно и всесторонне взвешивать применяемые идеи и принципы процесса внедрения информационных технологий, значение и результаты которых могут оказать неоднозначное влияние на развитие человеческого общества.

3. Всякий раз в решении возникающих этических вопросов использовать возможность применить уже существующие моральные принципы, законы, правила или этические практики, регулирующие поведение человека в обществе.

4. В том случае, если этически принятые прецеденты, традиции и политические курсы недостаточны для урегулирования вопроса или разрешения ситуации, Винер призывал, руководствуясь целью жизни человека, использовать великие принципы справедливости, чтобы найти решение, которое бы насколько возможно подходило этическим традициям данного общества.

Здесь, на наш взгляд, автор весьма верно излагает мысль о том, что нормы общественного бытия в обществе, строящемся на применении информационной технологии, должны быть заданы исходя из системы ценностей, которая, прежде всего, сохраняет духовные, нравственные, общечеловеческие ценности и общественные идеалы. Основы подобного общества базируются на таких фундаментальных понятиях, как

свобода, равенство, солидарность, толерантность и общая ответственность.

В конце 1940-х годов Н. Винер сделал ясное заключение о том, что интеграция в общество изобретенных вычислительно-информационной технологии приведет к координатным изменениям, что повлияет на все сферы жизни человека. Он предупреждает, что понадобятся десятки лет постоянных усилий для формирования и утверждения осмысленной системы ценностей нового общества. Автор абсолютно прав: нельзя допустить, чтобы новая информационная технология снабдила людей социальными ориентирами, «не слышавшими о важности добра и зла»[1]. Сегодня информационная этика представляет собой область междисциплинарного исследования и включает рассмотрение технических, моральных, юридических, социальных, политических и философских вопросов. Ее главная задача по-прежнему со времен Н. Винера заключается в конкретизации моральных норм с целью регулирования человеческого поведения в сфере создания и использования информационных технологий. Заложенное им метафизическое и научное основание для информационной этики продолжает давать глубокое и эффективное руководство для понимания и решения этических проблем, вызванных информационной технологией всех видов.

На наш взгляд, Н. Винер заложил основы новой ветви этики, которая позднее и была названа информационной этикой. В данном ключе мы особо подчеркиваем, что сформулированные ученым принципы теории информационной этики послужили почвой для дальнейших разработок, определяя важные характеристики этики будущего информационного общества: ее онтоцентричный характер, глобальность и значение в межкультурном диалоге современных цивилизаций.

[1] Винер Н. Кибернетика или управление и связь в животном и машине. М. : Советское радио. 1958. С. 27.

Далее, мы выделяем второй этап формирования информационной этики, который начинается с увлеченных дебатов об уникальности проблем в сфере применения компьютерной технологии и связан с именами В. Манера, Д. Джонсон, Дж. Мура и других пионеров компьютерной этики, исследующих вопросы в данной области.

В 1976 году В. Манер пришел к выводу, что введение компьютеров во многие сферы жизни общества, порождает совершенно новые этические проблемы, «которые, возможно, вообще не существовали бы, если бы не было компьютеров»[1]. Д. Джонсон придерживается другого мнения. Она исключает вероятность того, что компьютеры создают совершенно новые этические проблемы, с которыми общество никогда не сталкивалось. Компьютеры на самом деле лишь видоизменяют старые этические проблемы, то есть «дают им новый смысл»[2]. Например, рассматривая новые способы «инструктирования» действий человека при помощи информационных технологий или поиска ответов на подобные вопросы, как, например, должно ли быть защищено законом владение программным обеспечением? Или, представляют ли опасность для частной жизни человека огромные базы данных личной информации? В действительности они являются «новыми видами старых этических вопросов»: защита частной жизни, владение интеллектуальной собственностью и т. д. Мнение Д. Джонсон сосредоточено на том, что они не представляют собой совершенно новые этические проблемы, требующие дополнения к традиционным этическим теориям, как заявляет В. Манер.

Необходимо отметить, что дебаты В. Манера и Д. Джонсон положили начало продуктивным сериям научных ком-

[1] Maner W. Unique Ethical Problems in Information Technology, in T. Bynum and S. Rogerson (eds.). Science and Engineering Ethics // Global Information Ethics. – 1996. № 2 (2).

[2] Johnson D. Computer Ethics. New Jersey: Prentice-Hall. 2001. P. 76.

ментариев и публикаций о природе и уникальности компьютерной этики, привлекая новых исследователей в данную область. Так, отрывок, взятый из основного доклада В. Манера, вызвал активное обсуждение в научной среде: «Я пытался показать, что есть вопросы и проблемы, специфичные исключительно для компьютерной этики, поскольку для их существования необходимо наличие компьютерной технологии. Неспособность найти некомпьютерные аналогии свидетельствуют об уникальности этих вопросов. Отсутствие адекватной аналогии, в свою очередь, имеет моральные последствия. Обычно, когда мы сталкиваемся с незнакомыми этическими проблемами, мы применяем аналогии для построения концептуальных мостов в схожих ситуациях, с которыми мы сталкивались в прошлом. Затем мы пытаемся перенести моральные ситуации через мост, с аналогичной ситуации к настоящей ситуации. Отсутствие эффективной аналогии подталкивает нас находить новые моральные ценности, формулировать новые моральные принципы, развивать новые стратегии и также находить новые способы размышления над вопросами, встающими перед нами»[1]. «Уникальность дебатов» в течение десятилетий, которые последовали за этим отрывком, привели к значимым открытиям в изучении компьютерной и информационной этики в целом[2].

[1] Maner W. Unique Ethical Problems in Information Technology, in T. Bynum and S. Rogerson (eds.). Science and Engineering Ethics // Special Issue: Global Information Ethics. 1996. № 2(2). P. 152.

[2] Kocikowski A. Geography and Computer Ethics: An Eastern European Perspective, in T. Bynum and S. Rogerson (eds.). Science and Engineering Ethics // Global Information Ethics. 1996. № 2(2); Tavani H. The Uniqueness Debate in Computer Ethics: What Exactly is at Issue and Why Does it Matter? // Ethics and Information Technology. 2002. № 4(1); Tavani H. The Impact of the Internet on our Moral Condition: Do We Need a New Framework of Ethics? in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives. Albany: SUNY Press, 2005; Himma K. The Relationship Between the Uniqueness of Computer Ethics and its Independence as a Discipline in Applied Ethics // Ethics and Information Technology. 2003. № 5(4); Floridi L., Sanders J. The Foundationalist Debate in Computer Ethics, in R. Spinello and H. Tavani (eds.). Read-

Объяснить причину, по которой компьютерная технология поднимает такое большое количество этических вопросов, нежели использование каких-либо других видов технологии, пытается так же и Дж. Мур. Описывая природу компьютерной этики, он подчеркнуто употребляет выражение «компьютерная технология», поскольку убежден, что речь идет не только об использовании одного компьютера, но всей сопутствующей технологии – программного, аппаратного обеспечения и компьютерных сетей – в целом. Ответ на вопрос, почему компьютерная технология оказывает на общество и человека поистине революционное влияние, Дж. Мур видит в «логической пластичности» компьютера. Логическая пластичность компьютерной технологии, говорит Дж. Мур, позволяет человеку совершать большее количество действий, о которых он не имел представления. Отсутствие стандартов функционирования у ранее не применяемых практик Дж. Мур назвал «стратегическими вакуумами», впоследствии рождающими «концептуальные путаницы».

Таким образом, типичная проблема в компьютерной этике возникает из-за того, что есть стратегический вакуум в том, как компьютерная технология должна быть использована. «Компьютеры обеспечивают нас новыми возможностями, и те, в свою очередь, дают нам новые возможности выбора для действий. Главная задача компьютерной этики – определить, как должен поступать человек в подобных ситуациях, иначе – формулирование стратегии его действий… Единственная трудность состоит в том, что наряду со стратегическим вакуумом часто встречается концептуальный вакуум»[1]. На основании изложенного мы можем заключить, что меха-

ings in CyberEthics. – Sudbury, MA: Jones and Bartlett, 2004; Mather K. The Theoretical Foundation of Computer Ethics: Stewardship of the Information Environment, in Contemporary Issues in Governance. – Melbourne: Monash University, 2005; Bynum T. Flourishing Ethics // Ethics and Information Technology. 2006. № 8(4).

[1] Moor J. What Is Computer Ethics? // Metaphilosoph. 985. № 16(4). P. 266.

ническое применение этической теории для создания соответствующей стратегии в различных ситуациях не всегда возможно. Действительно, из-за того, что компьютерная технология предоставляет новые возможности для действий, формируются новые ценности.

В итоге указанных дискуссий была выделена новая ветвь прикладной этики, которую В. Манер предложил назвать «компьютерная этика». Он определяет новую область знаний как изучающую этические проблемы, «усугубленные, измененные или произведенные компьютерной технологией»[1].

Мы приходим к выводу, что третий этап становления новой этической области начинается в 1988 году с момента появления самого термина «информационная этика», который связывают с именами нескольких исследователей. Р. Гауптман использовал термин «информационная этика» на английском языке, рассматривая проблемы цензуры, неприкосновенности частной жизни, возможности доступа к информации, вопросы авторского права и добросовестного использования информации, аспекты формулирования кодексов этики[2]. Он описывает информационную этику в качестве динамичной и сложной научной области, изучающей принципы использования информации с моральной точки зрения, профессионального нейтралитета и социальной ответственности. На немецком языке термин «информационная этика» в том же году ввел Р. Капурро, призывая профессионалов в области информационных технологий к этическому регулированию процесса использования технологий[3]. В его представле-

[1] Maner W. Starter Kit in Computer Ethics. Hyde Park, N. Y. : Helvetia Press and the National Information and Resource Center for Teaching Philosophy. 1980. P. 15.

[2] Hauptman P. Ethical challenges in librarianship. N.Y. : Oryx press. 1988.

[3] Capurro R. Informationsethos und informationsethik – Gedankenzum verantwortungsvollen handeln im bereich der fachinformation [Information ethos and information ethics – Ideas to take responsible action in the field of information] // Nachrichten für Dokumentation. 1988. Vol. 39.

нии, именно понятие «информационная этика» наилучшим образом отражает условия современного общества. Третий ученый, использующий данный термин, также в 1988 году, – Г. Б. Де Майо, в работе по теме уголовного правосудия[1].

Важно отметить, что сформулированные Н. Винером основы теории информационной этики, на наш взгляд, послужили почвой для дальнейших исследований в данной области, определяя важные характеристики этики будущего информационного общества в качестве онтоцентрической теории глобального характера и межкультурного значения. Так, концепция теории Л. Флориди представляет информационную этику как онтоцентрическую науку[2], задача которой – оценить с моральной точки зрения всю существующую в мире информацию, в первую очередь, человека и его социальные взаимодействия в информационной среде. Р. Капурро видит задачу новой этики в качестве механизма, обеспечивающего гармоничное развитие человеческого общества на основе межкультурного диалога цивилизаций[3], подтверждая утверждение К. Горниак-Косиковской о глобальном характере и значении информационной этики как универсального инструмента при решении социальных и этических проблем всех видов и отношений[4]. Раскроем основные характерные особенности информационной этики, определяющие ее в качестве этики информационного общества.

---

[1] DeMaio H. B. Information ethics - It doesn't come naturally // Computer Security Journal. 1988. № 5(1).

[2] Floridi L. Information Ethics: On the Theoretical Foundations of Computer Ethics // Ethics and Information Technology. 1999. № 1(1); Floridi L. Internet Ethics: The Constructionist Values of Homo Poieticus, in R. Cavalier (eds.). The Impact of the Internet on our Moral Lives. Albany: SUNY Press. 2005.

[3] Capurro R. Towards an ontological foundation of information ethics // Ethics and Information Technology. 2006. Vol. 8. № 4.

[4] Kocikowski A. Geography and Computer Ethics: An Eastern European Perspective // Global Information Ethics. 1996. № 2(2).

Согласно теории Р. Капурро об истории развития взглядов информационной этики ее традиция от Древней Греции до начала XX века характеризуется двумя идеями: свобода слова; свобода печатных работ, или, в частности, свобода печати. Третий элемент возникает сейчас, в эпоху сетевого мира и электронной информации, а именно: свобода доступа, или право на общение в рамках цифровой среды[1].

Так, зарождение корней информационной этики необходимо искать в устной культуре Древней Греции. Данный процесс, прежде всего, связан с таким «продуктом» афинской демократии, как свобода слова (греч. паррезия). По мнению М. Фуко, свободное выражение правды о собственном бытии при определенных условиях становится моральным императивом. «Паррезия – речевая деятельность, в которой оратор выражает личное отношение к истине, он использует свою свободу и выбирает откровенность вместо убеждения, истину, а не ложь или молчание, риск смерти вместо жизни, критику вместо лести и нравственный долг вместо собственных интересов и моральной апатии»[2], – описывает М. Фуко.

На наш взгляд, в границах феномена информационной этики функция паррезии заключается в возможности позволить интерпретировать культурные традиции различных эпох и народов, оценить их взаимное влияние и общий вклад в практику нравственной жизни, а также научную и литературную рефлексию. Соответственно, для информационной этики идея паррезии несет важный смысл, поскольку позволяет обрести всеобъемлющее зрение в межкультурном диалоге цивилизаций.

[1] Capurro R. Towards an ontological foundation of information ethics // Ethics and Information Technology. 2006. Vol. 8. № 4.

[2] Foucault M. Discourse and Truth: the Problematization of Parrhesia. Berkeley: University of California. 1983.

Следующий этап, оказавший влияние на идеи информационной этики, протекает под влиянием книжной культуры. Эпоха Реформации, изобретение книгопечатания Гуттенбергом в 1455 году приносят идею свободы общения, подразумевая свободу общения в письменной и печатной форме. Далее Французская революция ведет к трансформации частных библиотек: доступ общественности к библиотечным фондам создает новое понимание свободы информации, который завершается принципом свободы прессы как одним из основ современной демократии.

Указанная третья идея в эпоху электронных коммуникаций начинает историю информационной этики три десятилетия назад в США под названием «компьютерная этика». Позже стечение этических проблем сферы компьютерных технологий с аналогичными вопросами из области журналистики, библиотековедения, управления и деловой этики, киберэтики, или интернет-этики, породило информационную этику в ее нынешнем виде.

С нашей точки зрения, современная история информационной этики связана, прежде всего, с возникновением проблем в области норм регулирования поведения человека в обществе, сформированном средствами массовой информации и компьютерной технологии. Подобная ситуация принимает драматический поворот с появлением сети Интернет как горизонтальной, неиерархической, интерактивной и глобальной среды для производства информации, хранения, распределения и обмена. При этом рассматриваемые информационной этикой вопросы гораздо шире, чем просто проблемы, порожденные в среде Интернет. Она занимается вопросами «цифровизации»[1], то есть реконструкции всех возможных явлений реального мира в качестве цифровой информации, и

[1] Capurro R. Towards an ontological foundation of information ethics // Ethics and Information Technology. 2006. Vol. 8. № 4. P. 176.

проблемами, вызванными процессами ее обмена, комбинации и утилизации.

Так, изучая смысл человеческого существования в цифровом измерении, в рамках теории цифровой онтологии, Р. Капурро вводит понятие «этоса» или, иначе, «бытия-в-мире с другими». В результате чего для него основной этический вопрос начинает звучать следующим образом: «Что следует улучшать в инфосфере для бытия-в-мире с другими?»[1].

В ходе исследования истории информационной этики, на наш взгляд, важно подчеркнуть: невозможно быть абсолютно уверенным в том, что в глобальном информационном обществе основание этики, особенно информационной этики, лежит преимущественно в западной традиции. В попытке создать подлинный диалог об этических ценностях в мультикультурном мире Интернета нельзя быть связанным исключительно предлагаемыми западным обществом убеждениями и традициями. «Точка зрения восточной философии на этические дилеммы, например, китайской или индийской, возможно, будет не менее эффективна и внесет собственный вклад в их решение. Речь не идет о превосходстве западного подхода»[2].

Мы убеждены в том, что истинно межкультурная информационная этика сочетает методологию различных мировых культур, независимо от своих исторических традиций, не исключая даже самые оригинальные пути. В данном ключе необходимо еще раз обратиться к плодотворному диалогу «паррезии» с традициями нравственной жизни и моральной философии Востока – гармонией, уважением, вежливостью.

[1] Capurro R. Intercultural information ethics // Paper presented at International ICIE Symposium 2004: Localizing the Internet: Ethical issues in intercultural perspective. 2004. Vol. 4.

[2] Capurro R. Intercultural information ethics // Paper presented at International ICIE Symposium 2004: Localizing the Internet: Ethical issues in intercultural perspective. 2004. Vol. 4. P. 31.

В свою очередь, Р. Капурро, рассматривая некоторые этические аспекты информационных технологий, предлагает опираться на философские традиции Африки. Например, один из этических принципов концептуальной деколонизации коренных народов «Ubuntu», то есть принцип совместного использования и заботы друг о друге. На основе чего он формулирует идею «быть человеком», которая предполагает признание и установление в обществе гуманных уважительных отношений, отчего в выборе между богатством и сохранением жизни другого человека первостепенно последнее. Отметим, что прозвучавшие идеи одновременно схожи с религиозными заповедями, которые отражены в положениях Всеобщей декларации прав человека ООН и олицетворяют классические моральные принципы.

В результате межкультурная информационная этика представлена как область, исследующая моральные вопросы отражения различных культурных традиций в информационной среде, поэтому мы подчеркиваем, что освоение современных информационных технологий – это не просто техническая, а скорее, культурная деятельность. Осмысление последствий цифровой глобализации открыло осознание разницы между цифровым и физическим миром, а также культурными аспектами человеческого существования. Сегодня вопрос о том, как информационные и коммуникационные технологии влияют на человеческую культуру, является ключевым с точки зрения философии и этики. Все существующие дебаты в области информационной этики, на наш взгляд, служат доказательством одной мысли: насколько глубоко использование информационной технологии может влиять на нравственную жизнь и культурные традиции человека. Информационная этика – открытое пространство, на котором должен проходить межкультурный диалог в поиске путей решения проблем современного общества.

В свою очередь, поддерживая идеи о важности межкультурного диалога в ходе развития информационной цивилизации, основываясь на теории Н. Винера о необходимости принятия постулатов информационной этики как этики будущего общества, К. Горниак-Косиковска аргументировано доказала, что компьютерная этика со временем развернется в глобальную этику, применимую в каждой культуре на земле[1]. При этом важно отметить, что К. Горниак-Косиковска в теории глобальной информационной этики не сформулировала существенных концепций и принципов, на которых должна базироваться информационная этика, она просто прогнозировала, что данная теория неизбежно появится ввиду глобальной природы Интернета и этических диалогов культур мира.

Согласно данной «гипотезе», региональные этические теории, такие как европейские утилитаристы и кантианские системы, так же как различные этические системы, вложенные в другие культуры мира, происходящие из «местных» историй и традиций, не всегда могут быть в полной мере применимы к этическим ситуациям формирующегося сегодня информационного общества.

В это же время информационная этика, обладает необходимым потенциалом для формирования глобальной этики, пригодной для Информационного Века. Новая этическая теория возникает из компьютерной этики в ответ на компьютерную революцию, кроме того, сама природа компьютерной революции показывает, что этика будущего будет иметь глобальный характер. Глобальный в пространственном смысле, так как она охватит весь земной шар. Глобальный так же и в том смысле, что она будет адресована всей совокупности че-

[1] Kocikowski A. Geography and Computer Ethics: An Eastern European Perspective, in T. Bynum and S. Rogerson (eds.), Science and Engineering Ethics // Global Information Ethics. 1996. № 2(2). P. 177-187.

ловеческих действий и отношений. Здесь вполне уместно провести аналогию с компьютерными сетями, имеющими глобальный характер, точно и информационная этика посредством тех же самых сетей должна распространиться по планете и стать принятой и понятной для каждого пользователя в его деятельности. В то же время, правила компьютерной этики, независимо от того, насколько хорошо продуманы, будут неэффективными, пока не будут признаны подавляющим большинством. Другими словами, компьютерная этика будет «универсальной, глобальной этикой»[1].

События, произошедшие после 1996 года прошлого столетия в сфере развития информационных технологий, стали подтверждением вышеназванных выводов, а заложенное в них Н. Винером фундаментальное основание послужило началом развития других исследований в данной области, в частности, информационной этической теории, или онтоцентричной теории этики Л. Флориди[2].

Разрабатывая свою информационную этическую теорию, Л. Флориди аргументировал, что существующая этика в целом должна быть расширена, чтобы включать намного больше, чем просто людей, их действия, намерения и характеры. При этом информационная этическая теория отличается от других более традиционных западных теорий, так как она не направлена заменить их, но, скорее, дополнить их этическими концепциями и взглядами, которые способны более широко рассмотреть информационно-этические ситуа-

[1] Kocikowski A. Geography and Computer Ethics: An Eastern European Perspective, in T. Bynum and S. Rogerson (eds.), Science and Engineering Ethics // Global Information Ethics. 1996. № 2(2). P.187.

[2] Floridi L. Information Ethics: On the Theoretical Foundations of Computer Ethics // Ethics and Information Technology. 1999. № 1(1); Floridi L. Internet Ethics: The Constructionist Values of Homo Poieticus, in R. Cavalier (eds.). The Impact of the Internet on our Moral Lives. Albany: SUNY Press. 2005.

ции, возникающие в современном обществе, нежели традиционные теории.

Термин «информационная этика» касается всего, что существует в качестве «информационных» объектов или процессов, своей совокупностью формирующими Вселенную в целостный организм – «инфосферу». Истолковывая каждый существующий объект в мироздании как «информационный» с минимальной моральной ценностью, информационная этическая теория может дополнить традиционные этические теории и идти дальше этого, перемещая фокус этического внимания с действий, характеров и ценностей человеческих агентов на «зло» (вред, вымирание, уничтожение) – «энтропию», вызванную объектами и процессами в инфосфере. С таким подходом каждый существующий объект – люди, животные, растения, организации, даже не живые артефакты, электронные объекты в кибернетике, части интеллектуальной собственности – может быть интерпретирован как потенциальный агент, влияющий на других, и как возможный пациент, подвергаемый влиянию других объектов.

Теория Л. Флориди, вкладывая в основание всех взаимодействий информационных объектов, прежде всего, доброту, предполагает следующие результаты:

- создание методов приложения нравственных критериев к кардинально увеличивающемуся количеству технологий и агентов в человеческом обществе (киборгам, роботам и т. д.);

- выработку адекватных моральных ориентиров в процессе взаимодействия внутри таких сложных социальных агентов, как правительственные структуры, различные организации и т. д.

Таким образом, Н. Винер был прав, когда предсказывал возникновение общества, которое будет нуждаться в этических правилах и процедурах для управления искусственными агентами. И современный социум сейчас уже соответствует такому описанию.

Кроме того, в теории Л. Флориди выделены следующие четыре класса свойств основных ценностей информационной этики: 1) модальный; 2) гуманитарный; 3) иллюстрирующий; 4) конструктивистский.

Модальный класс свойств информационной этики включает такие ценности, как логичность и осуществимость. Гуманитарный класс имеет дело со стабильностью и нестабильностью, безопасностью, доверием, конфиденциальностью, аккуратностью, искренностью и честностью. Класс разъясняющих свойств содержит понятия доступности и недоступности информации, возможности ее использования, ее систематичности. Наконец, конструктивистский класс характеризуется категориями моральности информации, ее современности, нормативности, в том числе избыточности. На наш взгляд, именно этот четвертый класс свойств отличает информационную этику от компьютерной этики. Конструктивистский класс свойств информации не имеет прецедента в истории культуры, поскольку гарантирует информационной сфере возможность различных форм расширения и изменения.

Информационная этика ориентирована на объект (субъект), отчего и является нестандартной онтоцентричной теорией, которая организована вокруг понятий рачительности и заботливости (for the sake and care). Вопросы всех видов нормативной этики «Что я должен делать?» или «Кем я должен быть?» заменяются здесь вопросом «Что следует уважать и улучшать?»[1]. В данном случае мы поддерживаем автора, поскольку самые простые, самоочевидные, признаваемые всеми людьми истины морали здесь поднимаются до

[1] Галинская И. Л., Панченко А. И. Компьютерная этика, информационная этика, киберэтика (Этико-правовое пространство информационно-компьютерных технологий) // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. М. 2003. С. 130.

уровня исторической перспективы, тех высших и конечных целей, вне отнесенности к которым человеческие поступки и институты лишаются смысла. В итоге, главная цель информационной этики заключается в оценке долга рационального индивида в терминах расширяющейся информационной сферы.

Таким образом, современная информационная этика имеет свои этико-философские истоки. Теория информационной этики формировалась под влиянием этики добродетели Аристотеля, деонтологической концепции И. Канта и этики утилитаризма. Сегодня наследие этих принципов и представлений о моральном поведении, заложенное в систему постулатов этического анализа, позволяет наиболее эффективно оценить модели и методы взаимодействия субъектов информационного общества.

В истории формирования информационной этики нами выделены три этапа, неразрывно следующие за развитием компьютерной технологии и возникновением сети Интернет. Первый этап развития новой информационной этики связан с именем Н. Винера, который в середине 40-х годов XX века предсказал новые этические проблемы, грядущие вслед за внедрением электронных компьютеров. Второй этап начинается с обоснования в 1976 году теории компьютерной этики в качестве отдельной философской дисциплины, изучающей этические проблемы в сфере использования компьютерной технологии. Третий этап сводится к появлению непосредственно самого термина «информационная этика» в 1988 году, в период бурного развития глобальной коммуникационной сети Интернет.

Кроме того, сформулированные Н. Винером основы теории информационной этики послужили почвой для дальнейших исследований в данной области, определяя важные характеристики этики будущего информационного общества в качестве онтоцентрической теории глобального характера и

межкультурного значения. Информационная этика как онтоцентрическая наука ставит перед собой задачу оценить с моральной точки зрения всю существующую в мире информацию, в первую очередь, о человеке и его социальных взаимодействиях в информационной среде. Новая этика представляет собой механизм, обеспечивающий гармоничное развитие человечества на основе межкультурного диалога цивилизаций, а также является универсальным инструментом при решении социальных и этических проблем всех видов и отношений, возникающих в обществе, основанном на информационных технологиях.

Исследование показало, что возникновение информационной этики не является чем-то неорганичным или случайным в современном социальном пространстве, организованном информационной технологией. Основные этапы становления информационной этики нераздельно связаны с развитием информационных технологий и социально-культурной трансформацией общества, ее этико-философские истоки и сформировавшиеся характеристики позволяют определить методологию решения многих социальных и этических проблем информационного общества, вызванных влиянием масштабного применения технологических достижений во всех сферах жизнедеятельности и смещением системы ценностей.

В свою очередь, дать наиболее ясное представление о том, как информационная этика формирует нравственное сознание социального субъекта в своеобразный нормативный порядок знаний, регулирующий общественные отношения в информационной среде, нам позволит системный метод, раскрывающий взаимосвязь внутренних и внешних отношений новой области этического знания современного социума.

2.2. ИНФОРМАЦИОННАЯ ЭТИКА КАК СЛОЖНАЯ СИСТЕМА

Рассмотрим феномен информационной этики с точки зрения системного подхода – универсального механизма, позволяющего изучить объект на более глубоком уровне и всесторонне. Системный подход, или системный метод, по описанию Г. И. Рузавина, представляет собой целостное исследование совокупности объектов (материальных, идеальных), при котором проявляются новые интегральные свойства взаимодействия составляющих объектов системы[1]. В отличие от других основных подходов, составляющих системное направление, – структурализма и структурно-функционального анализа, – центральным понятием в системном методе является «система».

Необходимо отметить, что смысл термина «система» каждая наука интерпретирует по-своему. В свое время П. Гольбах, объясняя объективную природу взаимосвязи явлений системы, придал данному понятию философский характер[2]. Ядром философской системы Г.В. Лейбница является монадология. Монаду он рассматривает как первичный, простой элемент, из которого составляется все сложное[3]. И. Кант увидел в понятии «система» гармонию и единство[4]. Ф. Энгельс развил представления о системе как о взаимосвязи тел[5]. В нашем случае будем придерживаться следующего

[1] Рузавин Г. И. Методология научного исследования. М. : ЮНИТИ-ДАНА, 1999. С. 275.
[2] Гольбах П. Система природы, или о законах мира физического и мира духовного. М. : ОГИЗ. Соцэкгиз, 1940.
[3] Лейбниц Г.-В. Сочинения: в 4 т. Т. I. М. : Мысль. 1982. С. 413.
[4] Кант И. Сочинения: в 8 т. М. : Чоро. 1994. Т. 3. С. 502
[5] Маркс К., Энгельс Ф. Соч. М. : Гос. изд-во политической литературы. 1955. Т.6. С. 442.

определения: «система – это совокупность элементов, образующих целостное единство»[1].

Поскольку специфика прикладной этики ориентирована на изучение практических проблем нравственного бытия, а целью является конкретизация моральных принципов применительно к определенным ситуациям, соответственно, сущность информационной этики заключена в определении норм и принципов действий субъектов относительно ситуаций, возникающих в процессе создания и использования информационных технологий. Опираясь на данное предположение, на основе анализа основных концепций информационной этики, исследующих круг актуальных задач и проблем изучаемой области, определим разделы системы информационной этики.

Так, с целью конкретизации задач информационной этики К. Химма и Г. Тавани разбирают круг тем, охватываемый новой этической теорией[2], в результате чего определяют следующие:

- обеспечение конфиденциальности и безопасности информации;
- вопросы интеллектуальной собственности;
- регулирование и управление сети Интернет, виртуальной реальности;
- область компьютерного моделирования и робототехника;
- профессиональная ответственность специалистов в области информационных технологий, журналистов, библиотекарей, специалистов из сферы биологии и медицины, занятых исследованиями на основе информационных технологий, представителей сферы бизнеса;

[1] Цырендоржиева Д. Ш. Системный подход: сущность и возникновение. М. 2001. С. 87.

[2] Himma K., Tavani H. The handbook of information and computer ethics. New Jersey: Wiley-Interscience. 2008.

- проблемы цензуры и доступ к информации.

На наш взгляд, представленные проблемы целесообразно объединить в группы, например, вопросы обеспечения конфиденциальности и безопасности информации, проблемы цензуры, доступа к информации являются предметом внимания компьютерной безопасности, конечная цель которой – защита информации в автоматизированных системах. В данную группу необходимо добавить задачи из области интеллектуальной собственности, точнее незаконного тиражирования информации. Второй ряд исследуемых задач информационной этикой складывается из проблем (этических, социальных и т. д.) применения достижений компьютерного моделирования и робототехники, которые дополняют уже представленную категорию вопросов профессиональной ответственности специалистов, обязанных прогнозировать возможные последствия приложения своих технологических изобретений. Третья группа проблем информационной этики в рассматриваемой работе охватывает вопросы обеспечения безопасности, возникающие в процессе взаимодействия посредством Интернет-технологий.

В отличие от описанного выше исследования, Дж. Лэдд выделяет две группы проблем в области информационной этики[1]. Он проводит разграничение между «макроуровнем» и «микроуровнем» этических вопросов, вызванных использованием информационных технологий в современном обществе. Первая группа связана с общими социальными последствиями применения информационных технологий, она включает в себя проблемы цифрового неравенства, свободного потока информации, конфиденциальности, вопросы профессиональной ответственности работников СМИ и т. д.

[1] Ladd J. The quest for a code of professional ethics: an intellectual and moral confusion. In Johnson D.G., Snapper J. W. (eds). Ethical Issues in the Use of Computers. Belmont: Wadsworth. 1985.

Важно добавить, что поддерживая данную теорию, М. Кохен вносит существенный клад в ее развитие. Он дополняет круг «макроэтических» проблем шестью этическими дилеммами общества, основанного на технологии[1]. Кратко обозначим их:

1. Безопасность и информация. Разрыв между экспертными знаниями и уровнем информированности общества в вопросах, касающихся обороны и безопасности. Проблема юридической защиты информации в межграничном потоке данных.

2. Занятость и информация. Этическая дискуссия относительно технологических изменений и организации работы различных специалистов.

3. Бизнес, промышленность и информация. Политические и экономические конфликты сторон, участвующих в формировании информационного общества.

4. Планирование. Контроль сложных компьютерных систем, экологические кризисы, институциональные изменения, проблемы социального здоровья населения и т. д.

5. Децентрализация. Этические аспекты коллективной работы в международных сетях, влияние потенциала и мощи технологий на человека.

6. Информационная перегрузка. Вопросы новых форм представления и обработки знаний. Эпистемологические и этические дискуссии о последствиях исследований и разработок в области искусственного интеллекта. Проблемы культуры и информационного колониализма. Темы о неприкосновенности частной жизни и целостности информации.

Определив глобальный характер исследований в области информационной этики, М. Кохен делает важное замечание: информация и знания, уравновешенные человеческими ценностями, обязаны справиться с описанными дилеммами, по-

[1] Kochen M. Information and society // Annual Rev. Sc. Techn. 1983. № 18.

скольку одних технических решений и профессиональных навыков недостаточно.

В свою очередь, в рамках данной теории микроэтическими проблемами названы те, которые возникают внутри группы информационных профессионалов и различных категорий пользователей, распространителей, производителей специализированной информации. Вот некоторые из них: проблемы доступности, безопасности данных, авторского права и вопросы ответственности профессионалов в области информационных технологий (этика исследований, обучения и информационной работы) и т. д. Здесь Дж. Лэдд поднимает вопрос о роли этики и профессиональных ценностей в кодексах практики, с целью обсуждения профессиональных этических проблем, с которыми сталкиваются специалисты.

Со своей стороны, конкретизируем круг проблем, составляющих категорию «микроэтических» вопросов: тема компьютерной безопасности (нарушение конфиденциальности, полноты и точности информации), вопросы авторского права, проблемы конкуренции на информационном рынке.

На основе изложенного выше мы можем заключить, что помимо проблем обеспечения классических принципов информационной безопасности (доступности, целостности, конфиденциальности информации), информационная этика охватывает вопросы культурного, политического, экономического, психологического характера, возникающие в глобальных сетях. Решение широкого спектра научных задач (экологических, образовательных и т. д.) так же попадает в поле ее зрения. На наш взгляд, представленная классификация задач в области информационной этики, характеризует ее как одну из важнейших научных дисциплин современного общества, обеспечивающей устойчивое функционирование всех сфер жизнедеятельности социума.

Изучая информационную этику как прикладную науку, Р. Капурро[1] также выделяет ее актуальные вопросы, требующие своего разрешения:

• проблемы моральной регуляции в сети Интернет, интернет-мифы;

• вопросы, возникающие в области использования компьютерной технологии;

• этические аспекты исследований в сфере медицины и биологии;

• этическое регулирование деятельности средств массовой информации;

• этические вопросы в сфере библиотечного и информационного обслуживания;

• морально-нормативное регулирование в информационной бизнес-среде.

С нашей точки зрения, в рассматриваемой теории задачи информационной этики не обладают таким глобальным характером, как отражает их М. Кохэн, но в то же время они отличаются высокой степенью конкретности, что позволяет ясно представить возможные методологические решения их реализации. В этой связи, мы определяем следующий круг вопросов, изучаемый в данной работе: решение проблем в области компьютерной технологии, задачи моральной регуляции в глобальной сети и этические аспекты деятельности специалистов, использующих в своей профессиональной практике информационные технологии (СМИ, медицина, библиотечное обслуживание и т. д.).

Таким образом, рассмотрев актуальные проблемы в теории информационной этики, обобщим их и обозначим основные разделы, изучаемые прикладной дисциплиной. На наш взгляд, классификация задач информационной этики выглядит следующим образом:

[1] Capurro R. Information ethics // CSI-communication. 2005. Vol. 28. № 12.

- решение проблем в сфере использования компьютерных технологий;

- решение этических и социальных проблем в киберпространстве или глобальной сети;

- изучение вопросов моральной ответственности специалистов родственных профессий (библиотекарей, журналистов и т. д.).

Приведенные выше проблемы информационно-этического характера, по нашему мнению, в первую очередь связаны с отсутствием ясного представления об этических ограничениях использования современных технологий, а также с непониманием выбора необходимых действий обществом и человеком при предоставлении новых возможностей.

Относительно первого раздела проблем в сфере компьютерных технологий стоит сказать, что изучением и анализом социального и этического влияния компьютерных технологий на все сферы общественной жизни занимается компьютерная этика – область философского исследования, изучающая моральные вопросы, связанные с процессом разработки, применения и использования компьютеров[1].

Сегодня термин компьютерная этика употребляют в профессиональной этике компьютерных профессионалов, руководствующихся этическими кодексами внутри своей профессии. Компьютерная этика рассматривает влияние компьютерной и информационной технологии на ценности человека, используя концепции из философии, социологии, права, психологии и т. д. Специалисты-практики компьютерной этики нынешнего дня – будь они философами, программистами, социологами и другими учеными – имеют одну цель: интегрировать компьютерную технологию и ценности

[1] Moore A. Information Ethics: Privacy, Property and Power. Seattle: University of Washington Press. 2005.

человека так, чтобы технология продвигала и оберегала ценности человека, а не наносила им ущерб.

Что касается раздела этических и социальных проблем в киберпространстве или глобальной сети, важно отметить, что, начиная с момента возникновения и решения указанных вопросов, сформировались следующие направления, занимающиеся этическими исследованиями в области регулирования человеческого поведения в среде Интернет: интернет-этика, сетевая этика, киберэтика, нетикет, виртуальная этика. В результате чего специалисты стали говорить о ряде проблем терминосистемы и кодифицирования в сфере этического регулирования применения информационных технологий, которые нуждаются в значительной степени уточнения. На наш взгляд, существует необходимость внести некоторую ясность в сложившуюся ситуацию.

Сетевую этику связывают с принципами становления культуры поведения сети Интернет. По аналогии с традиционной профессиональной этикой здесь выделены основные слагаемые сетевой этики: кодекс сетевой этики (регулятор отношений в Сети) и сетевой этикет (регулятор поведения в Сети).

Термин «нетике́т» (или «сетике́т») возник в результате слияния слов «сеть» (англ. net) и «этикет». Значения слов, составляющих термин, предполагают, что данное понятие характеризует правила поведения в сети Интернет, которых придерживается большинство интернет-сообществ[1]. Данный термин впервые встречается в 80-х годах XX века в международной любительской компьютерной сети FIDO, положившей начало развитию социальных форумов.

Виртуальная этика связана с осмыслением проблем интернет-коммуникаций. Рассматривая глобальную сеть Интернет в качестве социального электронного пространства,

[1] Shea V. Netiquette. San Francisco: Albion Books. 1994.

специалисты выделяют ее многофункциональность. В первую очередь, это масштабное коммуникационное поле, состоящее из собственной реальности: развлечения, деловая среда, виртуальные сообщества, интернет-мифы и интернет-конфликты, а также вытекающие отсюда социальные, креативные и асоциальные последствия виртуальных игр[1].

Киберэтика призвана регулировать поведение человека в информационном мире. Она «имеет дело с будущими компьютерными технологиями, с качеством жизни, с этическими и социальными проблемами, связанными с киберпространством и обществом всемирной компьютерной сети (networked society)»[2]. Впервые термин «киберпространство» был введен У. Гибсоном в фантастическом романе «Нейромант» [3], под термином подразумевалось виртуальное пространство, состоящее из ресурсов, доступных через компьютерные сети.

Киберэтику также называют интернет-этикой, то есть областью прикладной этики, изучающей этические вопросы и моральные дилеммы, связанные с появлением цифровых технологий и глобальной виртуальной среды, в частности: проблемы конфиденциальности, точности и доступности информации, защиты интеллектуальной собственности, безопасности данных и цифрового неравенства[4].

---

[1] Скворцов А. А. Мораль и современные информационные технологии [Электронный ресурс]. Режим доступа: URL: http://iph.ras.ru/uplfile/ethics/RC/prog/applied/IP.html (дата обращения: 20.03.2014).

[2] Галинская И. Л., Панченко А. И. Компьютерная этика, информационная этика, киберэтика (Этико-правовое пространство информационно-компьютерных технологий) // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. М. 2003.

[3] Гибсон У. Нейромант. М. : Аст; СПб : Terra Fantastica. 2000.

[4] Baird R., Ramsower R., Rosenbaum S. Cyberethics: Social & Moral Issues in the Computer Age. Amherst, N. Y. : Prometheus Books. 2000. P. 124.

Все перечисленные выше понятия, то есть сетевую этику, нетикет (сетикет), виртуальную этику, киберэтику и интернет-этику, некоторые специалисты видят в качестве фрагментов единой теории[1], что, на наш взгляд, весьма верно. Исследуемые направления изучают проблемы социального, этического характера, возникающие в процессе взаимодействия в компьютерной сети. Далее в нашем исследовании указанное направление научного исследования будем назвать «киберэтикой», иначе – этикой, изучающей проблемы информационного взаимодействия в компьютерной сети или в киберпространстве.

Под киберэтикой, как правило, понимаются правила нравственного (т. е. правильного, честного, справедливого) поведения в глобальной среде. Она простирается далеко за пределы «сетевого этикета» – правил, выработанных в ранний период использования Интернета. Киберэтика распространяется на коммуникативные (чаты, форумы, блоги и др.) и некоммуникативные сервисы: совместную работу, онлайновые игры, покупки или приобретение/продажу биржевых акций»[2]. Кроме того, данное этическое поле – предмет пристального изучения, так, А. Ю. Алексеевой[3] рассмотрены вопросы становления этики Интернета, С. В. Бондаренко[4] выделены социологические аспекты, И. Л. Галинской и А. И.

[1] Скворцов А. А. Мораль и современные информационные технологии. [Электронный ресурс]. – URL: http://iph.ras.ru/uplfile/ethics/RC/prog/applied/IP.html (дата обращения: 20.03.2014).

[2] Войскунский А. Е., Нафтульев А. И. Актуальные психологические проблемы киберэтики // Гуманитарная информатика. Томск. 2007. Вып. 3.

[3] Алексеева И. Ю. Этика Интернет. Internet Ethics. – Houndmills etc.: Macmillan press. 2000.

[4] Бондаренко С. В. Киберэтика и сетевые сообщества (молодежный аспект проблемы с точки зрения американских социологов и психологов) // Социальные и психологические последствия применения информационных технологий. М. 2001.

Панченко [1] –юридические вопросы, психологические проблемы – А. Е. Войскунским и др.[2]

В свою очередь, Дж. Мур конкретизирует содержание понятия «киберэтика», отмечая следующее: киберэтика формулирует и обосновывает политику в области этического использования компьютеров, точнее, решает вопросы компьютерной этики в киберпространстве. Р. Бэрд, Р. Рэмсовер и С. Розенбаум, говоря об общем характере проблем компьютерной этики и киберэтики, замечают, что, в отличие от компьютерной этики, киберэтика решает вопросы цензуры и фильтрации информационного трафика, свободы и благопристойности информации, а также интернет-зависимости и игромании[3].

Со своей стороны относительно сфер деятельности киберэтики подведем итог: изучаемые вопросы киберэтики и компьютерной этики во многом схожи, точнее, киберэтика исследует проблемы компьютерной этики, отражающиеся в глобальной Сети или киберпространстве. При этом сеть Интернет, благодаря своим уникальным характеристикам, порождает новые специфические этические вопросы, которые ищут своего разрешения в рамках киберэтики.

Третий раздел вопросов относительно моральной ответственности специалистов включает этические аспекты применения информационных технологий в различных профессиональных сферах. Здесь важно отметить, что исследование проблем моральной ответственности специалистов в рамках прикладной этики определяется как одна из актуальнейших

[1] Галинская И. Л., Панченко А. И. Этико-правовое пространство информационно-компьютерных технологий // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. М. 2003.

[2] Войскунский А. Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. №1(3) и др.

[3] Baird R., Ramsower R., Rosenbaum S. Cyberethics: Social & Moral Issues in the Computer Age. Amherst, N. Y. : Prometheus Books. 2000.

задач современного общества: «Идея освоения прикладных этик исходит из принципиальной важности качества «вхождения» этико-прикладного знания в мир профессиональных практик»[1]. При этом подчеркнем мысль, что в целях полноценной конкретизации парадигмы социальной ответственности профессионала, а также расширения потенциала версии прикладной этики важно выйти за пределы конкретной профессиональной сферы. В данном контексте моральные принципы информационной этики отражают позицию не только людей, находящихся в профессии, связанной с производством и использованием информационных технологий, но и тех, кто «не является членами этих профессий, кто находится вне их, но кто кровно заинтересован»[2] в том, какое решение найдут эти технологии.

Таким образом, мы выделяем следующие разделы, или подсистемы, составляющие систему информационной этики: компьютерная этика, киберэтика и вопросы моральной ответственности специалистов. Данные подсистемы в свою очередь можно рассматривать как системы.

С нашей точки зрения, в рамках компьютерной этики рассматриваются следующие актуальные темы:

- проблемы обеспечения безопасности информации: конфиденциальность, доступность и целостность;
- вопросы, касающиеся охраны интеллектуальной собственности, в первую очередь распространяющиеся на программные продукты;
- этические аспекты компьютерной безопасности: физические, программные атаки и т. д.;
- вопросы профессиональной ответственности специалистов из области информационных технологий.

[1] Бакштановский В. И., Согомонов Ю. В. Ойкумена прикладной этики: модели нового освоения. Тюмень: НИИ ПЭ ТюмГНГУ. 2007.
[2] Там же. - С. 18.

В сферу вопросов киберэтики относятся следующие темы:

- вопросы киберпреступности в глобальной сети, которая ставит под угрозу конфиденциальность, доступность, целостность информации;
- этические особенности и нравственные принципы общения в компьютерных сетях: например, свобода слова, наполнение контента, регулирование и саморегулирование интернет-сообществ, толерантность и т. д.;
- этические аспекты научной работы в сети Интернет, например, проблема плагиата, вопросы открытых или закрытых программных кодов и т. д.;
- изучение будущих этических и социальных последствий от внедрения новейших информационно-коммуникационных технологий посредством использования возможностей глобальной сети;
- проблемы интернет-зависимости и игромании;
- вопросы доступа и цензуры информации, правовые аспекты;
- проблемы цифрового неравенства;
- изучение механизмов реализации межкультурного диалога.

Еще раз важно отметить, что вопросы, составляющие разделы киберэтики и компьютерной этики, во многом схожи. На наш взгляд, в ряде моментов компьютерная этика соприкасается с киберэтикой, например, в таких вопросах, как качество веб-ресурсов, интеллектуальная собственность, цифровое неравенство и т. д., которые во многом сближают их между собой. Как было уже сказано ранее, киберэтика исследует проблемы компьютерной этики, отражающиеся в киберпространстве. При этом сеть Интернет, благодаря своим уникальным характеристикам, порождает новые специфические этические вопросы (цензура информации, кибер-

преступность, интернет-зависимость и т. д.), которые ищут своего разрешения в рамках киберэтики.

Далее, в границах третьего раздела системы информационной этики уточним профессиональные сферы, на которые должно распространяться этическое регулирование:

- профессии в области информационных технологий, от производителей до пользователей;
- информационно-библиотечное обслуживание;
- научные исследования на базе информационных технологий;
- журналистика и деловая сфера.

На основании перечисленного выше сделаем следующее заключение: данный раздел составляют все сферы деятельности, функционирование которых основано и/или активно протекает в поле использования информационных технологий, рождая этические и социальные вопросы относительно их применения. Для информационной этики в пределах описываемой подсистемы представляют интерес различные направления научной деятельности, которые связаны с исследованиями на базе информационных технологий в плане изучения этических и социальных аспектов внедрения, использования нанотехнологий и других высокотехнологичных разработок, проблемы искусственного интеллекта, генной инженерии, клонирования.

Кроме того, мы отмечаем важный момент: разделение указанных проблем в рамках составляющих разделов информационной этики носит условный характер, поскольку перечисленные вопросы тесно связаны и переплетены между собой, в результате чего четкие границы между сферами исследований дисциплин стираются.

Таким образом, система информационной этики содержит следующие компоненты:

Информационная этика в качестве сложной системы обладает иерархичной структурой, имеющей следующий вид. Основными разделами системы являются компьютерная этика и киберэтика, а также раздел вопросов моральной ответственности специалистов в области безопасного использования информационных технологий. Отметим, что структура обладает значимой ролью в организации системы. Она интегрирует и коммутирует элементы, тем самым порождая целостность и новые системные качества. При всей своей динамичности и подвижности, поскольку структура реагирует на изменения состава ее компонентов и их взаимодействие с внешней средой, она характеризуется определенной устойчивостью и самостоятельностью. Так, перечисленные компоненты нашей системы необходимо рассматривать в виде подсистем, обладающих относительной самостоятельностью. Под относительной самостоятельностью понимаются особые черты и характеристики, специфичные для каждой части системы. Подсистемы могут быть изменчивы и подвижны, могут перерасти в самостоятельную систему или часть других.

Каждый из разделов системы информационной этики (компьютерная этика, киберэтика, раздел вопросов моральной ответственности специалистов) содержит в своей струк-

туре следующие элементы: нормативную этику, ситуативную этику и профессиональную этику. В отличие от относительно самостоятельных частей системы, элементы отражают переход к низшему организационному уровню и представляют предел делимости. Задачи и особенности указанных элементов в конечном итоге и задают характер взаимодействия и функции частей системы в целом. Функция представляет собой отношение элемента к целому, направляющее его действия согласно заданным целям системы, тем самым сохраняя ее целостность[1]. Функция отражает деятельность или активность системы в целях достижения поставленных задач. В функциональной зависимости друг от друга находятся одновременно как отдельные компоненты нашей системы, так и компоненты с системой в целом.

Например, задача ситуативной этики в основном состоит в выработке практических рекомендаций применительно к конкретным ситуациям, возникающим в процессе применения информационных технологий. Ситуативная этика стремится сформулировать правила решения этических проблем, возникающих в сферах жизнедеятельности и общения человека на интимном (межличностном) и публичном уровне. Данное направление строится с использованием методов психологии, педагогики, знаний медицины и т. д., предполагает воспитательную и самовоспитательную работу. Составляющим ситуативной этики рассматривается этикет как внешнее выражение внутренней нравственной культуры личности. Этика межличностных отношений конкретизирует общие нравственные нормы в таких проявлениях, как этика дружбы, любви, этические проблемы субкультур, сообществ и моральные вопросы киберпространства.

[1] Райбекас А. Я. Вещь, свойство, отношение как философские категории. Томск: Томск. ун-т. 1977. С. 156.

В сфере информационной деятельности система морального воспитания личности и общества должна формировать естественную жизненную необходимость ориентации на соблюдение установленных в обществе норм и законов. Даже те общественные силы, которые резко расходятся между собой в понимании путей политических и экономических преобразований, интерпретации истории, должны сходиться в том, чтобы признавать мораль в качестве высшей точки отсчета человеческих приоритетов.

В этой связи мы выделяем следующие этические ценности, которые обязана утверждать информационная этика в рамках действия своих основных частей в качестве необходимых для безопасного сосуществования в информационной сфере:

1) каждый должен руководствоваться принципами равновесия и гармонии, контролировать свои поступки;

2) должен соблюдать установленные информационные нормы;

3) должен быть ответственным за свои поступки.

Нормативная этика как элемент, составляющий компьютерную этику, киберэтику и раздел вопросов моральной ответственности специалистов, призвана оценивать поступки членов информационного сообщества с точки зрения моральных позиций и формулировать нравственные предписания к конкретным действиям. Так, нормативная этика выполняет следующие функции: обосновывает и прокламирует ценности, кодифицирует нормы поведения, моральные качества человека, формирует нравственные убеждения и преобразовывает социальные императивы в личные импульсы.

Определенное представление о добре и зле свойственно каждой эпохе. Любая этическая система прошлого искала верный путь к блаженству: через сострадание, чистоту мысли, терпение и невозмутимость. Ускользающая истина между моральной обязанностью и ее практическим благоразумием

беспокоит умы философов разных эпох. Характеризуя процесс развития современных технологий, Н. Винер говорил, что какой бы совершенной ни была техника, использовать ее будет человек, потому что он есть та мера всех вещей, которые создают его дерзновенный разум и неуемная фантазия[1]. Человеку свойственно ошибаться и впадать в грех. Постулат нравственной философии – ничем не детерминированный выбор между добром и злом – определяет формальное «условие возможности» совершения этически значимого поступка.

Зло, как бы оно ни выражалось, заключается в эгоизме человека, в его стремлении к самоутверждению, к самообогащению за счет остальных и всего остального. «Абсолютное (в моральном смысле) благо не может сводиться ни к какому утилитарному благу, ни к какому обретению вещи, общественного положения, т. е. ни к чему из того, что обычно человек стремится достичь в повседневной жизни, ибо все эти блага не только разрушаются от их комбинирования со злом, но и очень часто являются соблазном к согласию по использованию средств, которые сами по себе являются моральным злом»[2]. На протяжении всей человеческой истории таким проявлениям человеческой культуры, как жадность, корысть, лицемерие, и всем другим подобным отведена существенная роль в составе мотивов, движущих человеческим поведением.

В сферу рассматриваемых вопросов нормативной этики входит определение «должного», она обосновывает выбор ценностных ориентиров общества. Нормативная этика рассматривает в нормативно-оценочной функции такие понятия, как «добро», «зло», «справедливость», «долг» и т. д., аргу-

[1] Винер Н. Творец и робот. М. : Пргресс, 1996. С. 63.
[2] Мусхелишвили Н. Л., Сергеев В. М., Шрейдер Ю. А. Ценностная рефлексия и конфликты в разделенном обществе // Вопросы философии. 1996. № 11. С. 18.

ментирует выбор поступка в ситуациях определенного типа, возникающих в ходе информационного взаимодействия.

Информационная этика, непосредственно через теорию и практику своих составляющих разделов, стремится определить такие качества, как уважение к праву, уважение к другим членам общества и к их интересам, доверие, честность, социальная ответственность.

В данном ключе подчеркнем исследовательский характер информационной этики, определяя ее следующие функции:

- изучение регулятивных механизмов, влияющих на информационные отношения в истории человеческой цивилизации;

- развитие рефлексии в информационном поле на моральные установки и традиции на индивидуальном и коллективном уровне;

- формулирование нормативных аспектов в виде этических кодексов.

На прикладную этику как элемент, составляющий основные разделы системы информационной этики, возложена серьезная обязанность – исполнять роль проектно ориентированного этического знания в обществе. Эта роль выражается в виде обеспечения «технологического» (моделирующего, экспертирующего, проектирующего, консультирующего и т. п.) потенциала этико-прикладных исследований и культивирования фронестической способности субъекта[1]. Сегодня разработаны и внедрены в практику основные технологии этико-прикладного знания:

1. Этическое проектирование (например, этической комиссии профессиональной ассоциации в «несудебном» – консультативном формате).

[1] Бакштановский В. И., Согомонов Ю. В. Ойкумена прикладной этики: модели нового освоения. Тюмень: НИИ ПЭ ТюмГНГУ. 2007. С. 24.

2. Этическое конструирование (например, конвенции профессиональных сообществ или миссии различных организаций).

3. Этическая экспертиза (общественная, гражданская; один из примеров – экспертиза проекта арктической политики).

4. Этическое консультирование ассоциаций и организаций (например, университета в ситуации самоопределения).

5. Этическое моделирование (серия этико-прикладных игр).

6. Технологии учебного (в рамках «этического практикума») и исследовательского «кейс-стади» (например, самопознание образовательной и журналистской корпораций).

При этом важный аргумент в пользу внедрения этических технологий прикладной науки связан с развитием в них потенциала испытания выбором. Здесь необходимо выделить игровое моделирование, являющееся элементом и экспертизы, и консультирования, и проектирования, и образования и т. д. Этико-прикладные игры – способ включения лиц и групп, принимающих решение, в ситуацию морального выбора, стимулирующую этическую рефлексию[1].

В рамках профессиональной этики выделим вопросы, на которые информационная этика обязана обратить особое внимание, включая свои составляющие:

- права человека и ответственность;
- интеллектуальная собственность;
- процессы сбора и классификации информации;
- доступ и распространение информации.

Также в аспекте профессиональной этики специалистов сформулируем задачи информационной этики, соответствен-

[1] Бакштановский В. И., Согомонов Ю. В. Ойкумена прикладной этики: модели нового освоения. Тюмень: НИИ ПЭ ТюмГНГУ. 2007. С. 25.

но, решение которых ложится на компьютерную и киберэтику:

- изучение возможных этических проблем в процессе использования информационной технологии;
- развитие чувства ответственности в отношении результатов труда;
- повышение квалификации специалиста путем изучения основ информационной культуры и принятия нравственных ценностей;
- информирование об этических аспектах работы и их роли в профессиональной деятельности.

Общей особенностью всех видов профессиональной этики является то обстоятельство, что в них высшие моральные ценности, сохраняя свое общечеловеческое значение, обретают вместе с тем некоторые особые черты. Специфичность понимания общечеловеческих моральных ценностей сказывается на особенностях проявления добра и зла в юридической практике, страдания и сострадания в медицине, долга и совести в военном деле и т. д. В основе информационной этики лежат такие категории, как безопасность и ответственность. Моральная ответственность – это отношение личности к окружающему миру, к обществу, характеризующаяся с точки зрения степени осуществления конкретных нравственных требований (добра, долга, чести и т. д.). Она выражает в то же время мировоззренческую и социально-политическую позицию личности. В этом случае важны как теоретические обоснования, так и практические интересы.

Сущность технологии находится в человеческой культуре. Повторим, что решающее значение в данной ситуации приобретают техническая грамотность, культура и этика поведения человека, которые должны соответствовать существующей модели информационной безопасности. Профессионалы отмечают, что исправная работа сложнейших технологически связанных между собой и потенциально опас-

ных систем и их сетей (в самом широком понимании) является необходимым, но недостаточным условием обеспечения информационной безопасности[1]. Такие объективные факторы, как технологии и их качество, реже являются причинами возникающих проблем, чаще ими являются субъективные факторы, например, степень ответственности специалиста. На Всемирном саммите по устойчивому развитию (Йоханнесбург, 2002 г.) Генеральный секретарь ООН Кофи Аннан сказал: «Все надежды Организации Объединенных Наций, всего человечества воплощены в одном слове, и это слово "ответственность"»[2].

Конечная цель практики всех этических исследований – способствовать развитию в человеке сознательной ответственности за свои действия, регулирующей все его поступки. В результате чего необходимо уделять значительное внимание философскому воспитанию, насаждать определенную социальную модель поведения в обществе. Формировать специалиста с активной жизненной позицией, для которой присуще следующее свойство – осознание ответственности за совершаемые действия и за их общественно значимые последствия. Этика рассматривает ответственность в ее нравственном содержании – как ответственность за поведение с точки зрения его соответствия признанным в данном обществе моральным ценностям. Именно через понятие ответственности теория морали получает непосредственный выход в практику общественной жизни. Поэтому сейчас, с пониманием того, что техника наносит огромный вред природе и человечеству, приходит осознание, что необходимо увеличить ответственность человека за то, какую технику он производит и как ею пользуется.

[1] Research on mitigating the insider threat to information systems // RAND. Conference Proceedings. 2000. August.
[2] The Earth Times. Johannesburg. 2002. 3 September. P. 3.

Принятие моральной ответственности – требование, общее для всех моральных систем. Выделены следующие три условия, которым должна отвечать общая моральная система:

- благо всего человечества как высшая ценность, ответственность не только перед нынешним, но и будущими поколениями;

- все моральные нормы и требования обращены ко всем без исключения;

- все моральные нормы и обязательства должны быть связаны с высшей ценностью: следуя этим нормам, субъект способствует человеческому благу.

Эти минимальные требования призваны исключить частные интересы и псевдоморальные обязательства во имя общей моральной системы, которая гарантирует общую ответственность каждого.

В вопросах моральной оценки действия в информационной сфере встает проблема свободного выбора поступков и их мотивов. Свобода морального выбора тесно связана с нравственными устоями общества, и эта связь имеет не только теоретическое, но и практическое значение. Информатизация должна регулироваться государством посредством установления общеобязательных правил, в которых учитываются моральные ориентиры, потребности и запросы гражданского общества.

В отличие от процессов, происходящих в природе, одна из особенностей человеческой деятельности заключается в том, что люди, прежде чем достигнуть какого-нибудь результата, предварительно создают его мысленную модель. Вместе с тем в истории постоянно наблюдается разрыв между поставленными целями и достигаемыми результатами, несоответствие между потребностями людей и продуктами их деятельности. Этот обесчеловеченный, вещный мир (включая и превращение духовных продуктов в «вещи», деньги и

другие материальные ценности), в котором отношения между людьми и результатами их деятельности «перевернуты». Человек из свободного субъекта своих отношений с миром и самим собой превращается в страдающий объект, является миром несвободы, социального отчуждения как господства над человеком не контролируемых им, враждебных социальных сил, продуктов собственной деятельности. Целью утилитарной технологии является полезность использования технологических достижений. Однако с точки зрения общей моральной системы полезность должна относиться к человечеству в целом – как к настоящему, так и к будущим поколениям. Это понятие следует отличать от полезности для отдельных групп – стран, научных сообществ, компаний и т. п., поскольку интересы групп могут не совпадать с интересами человечества в целом: производство нового оружия, основанного на информационных технологиях, может отвечать интересам отдельных групп, но вредно для человечества в целом.

Словом, мы разграничиваем общеморальный уровень полезности, с одной стороны, и частные представления о полезности – с другой. Поскольку ни коммерческие интересы, ни какие-либо обязательства не имеют ничего общего с моральными обязательствами в целом. Например, нация в лице правительства может считать оружие полезным для собственных интересов. Люди, вовлеченные в процесс его создания или использования, несут определенные обязательства перед страной, они могут считать его благом, однако их мнение не является общеморальным, поскольку служит интересам одной нации и игнорирует интересы всех остальных людей, которые могут оказаться жертвами этого оружия. История богата примерами, когда смешивают патриотизм с общеморальными нормами, тем самым отрицая свою ответственность перед человечеством. Это подобно тому, как по-

литики выдают обязательства перед нацией за общеморальные обязательства.

Если новое изобретение способствует улучшению условий жизни, то возможны два вида моральных аргументов «против». Во-первых, это улучшение может осуществляться за счет ухудшения других условий жизни (аргумент потерь и приобретений). Во-вторых, улучшение условий жизни может быть несправедливо распределено между людьми – за счет ухудшения условий жизни других людей (аргумент распределения). Если же улучшение действительно несет благо людям, то не существует общеморальных аргументов против его реализации. Необходимо всегда помнить о ситуациях, когда благие, но наивные намерения способны привести к отрицательным последствиям. Согласно принципу справедливости, необходимо такое распределение благ, когда никто не получает преимущества перед другими. Существует немало примеров, когда технические изобретения служили для удовлетворения потребностей привилегированного класса и в то же время способствовали ухудшению экологической обстановки, нанося ущерб каждому человеку. Поскольку сами по себе современные технологии не дают решения глобальных проблем, именно потому необходимы этические требования ее применения.

Далее необходимо заметить, что описанное отношение компонентов системы информационной этики позволяет выделить различные уровни, горизонтальные и вертикальные «срезы», находящиеся в подчинении системы и связанные между собой. Каждая ее подсистема в виде компьютерной или киберэтики имеет определенную степень автономии, то есть является одновременно и иерархичной и неиерархичной. Указанное свойство в известном смысле придает системе информационной этики своеобразную прочность. Данная характеристика при весьма диссипативном характере системы сохраняет ее целостность, позволяя оперативно и гибко отве-

чать на внешние раздражители. Сигналы, поступающие извне, вполне способны обрабатываться на нижних уровнях, тем самым не перегружая высшие уровни целостности. Функции каждой части сложной системы информационной этики заданы исходя из задач и особенностей составляющих ее элементов.

Информационная этика, согласно теории сложных систем, которые помимо иерархически образованных частей (подсистем) структуры обладают такими свойствами, как становление, существование и жизнедеятельность, также имеет относительно самостоятельные, но взаимосвязанные аспекты: свою историю, структуру и функционирование. При этом информационная этика развивается и за счет внутренних импульсов и противоречий, чем представляет самоорганизующуюся систему. Способность к саморазвитию и саморегулированию объясняется наличием в сложных системах специфических механизмов, ведущих к согласованию действий и интеграции компонентов системы. В самом общем смысле понятие самоорганизации предполагает внутреннюю упорядоченность.

Кроме того, информационная этика, исходя из определения Дж. Клира, открытая система, поскольку непосредственно связана с окружающей средой. Система испытывает постоянное воздействие как от социального окружения, так и природного, поскольку природа является объектом преобразовательной деятельности человека. Так, техника как продукт общественного производства становится действительной частью объективной реальности и, в конце концов, даже формирует ее модели.

В итоге мы можем определить основные цели информационной этики, задающие направления будущих исследований в рамках составляющих ее подсистем:

- продвижение нравственных ценностей в информационном обществе;

- развитие регулятивных механизмов в информационном поле;
- выявление скрытых противоречий в информационной теории и практике;
- разрешение этических и социальных конфликтов в информационной среде.

В результате освещенной проблематики данной области определим специфические черты, которые должны принадлежать информационной этике:

1) она должна быть более специализирована, что сделает ее более прагматичной;

2) она должна включать в себя не только теорию морали, но и комплекс внеэтических знаний о морали – социологических, психологических, педагогических и т. п.;

3) она должна обладать технологическим аспектом: выработка методов внедрения прикладного знания в практику в виде проектов, моделей, кодексов.

Таким образом, информационная этика – сложная и самоорганизующаяся система, обладающая иерархической структурой с характерными взаимосвязями ее компонентов. Ее основными разделами являются компьютерная этика и киберэтика, а также раздел вопросов моральной ответственности специалистов в области безопасного использования информационных технологий. Перечисленные компоненты системы необходимо рассматривать в виде подсистем, обладающих относительной самостоятельностью, каждая из которых в своей структуре содержит следующие элементы: профессиональную этику, ситуативную этику и нормативную этику. При этом мы отмечаем, что предлагаемое структурирование не может быть в полной мере однозначным и жестким, так как имеет условный характер, а его отдельные элементы переплетаются и взаимопроникают. Задачи и особенности составляющих подсистем в конечном итоге и задают характер взаимодействия и функции частей системы в це-

лом. Система информационной этики является открытой, функционирующей и развивающейся.

По нашему мнению, благодаря слаженной работе всех приведенных компонентов системы, согласно функциям каждого составляющего звена, информационная этика формирует особое нравственное сознание человека в своеобразный нормативный порядок знаний, регулирующий общественные отношения в информационной среде, тем самым обеспечивая решение поставленных задач информационной безопасности. Информационная этика призвана повысить компетентность социальных субъектов об их правах и обязанностях в информационном обществе. В результате чего, бесспорно, роль информационной этики в процессе обеспечения информационной безопасности выходит на первый план. Кроме того, такие категории, как «безопасность» и «ответственность», преобразуются в методологические основания социальных норм, регулирующих деятельность человека в информационном обществе.

Системный подход к изучению информационной этики, нового научного знания, имеет особое значение для социально-философского анализа информационной безопасности. Взаимосвязи частей информационной этики позволяют ясно представить то, что процесс развития общества на основе информационно-технологических преобразований, вызвавший появление на свет трех основных разделов нашей системы, целиком и полностью определен сознательным характером деятельности социальных субъектов, в которой отражены их непосредственные цели и ценности. В рамках информационной безопасности представленная зависимость является решающей в обеспечении эффективного и безопасного применения информационных технологий для социума и формирования общественных отношений в информационной сфере.

В качестве инструментальных оснований деятельности социальных субъектов информационная этика формирует свои принципы в области обеспечения информационной безопасности человека, общества, государства, которые рассмотрены далее. Система и принципы информационной этики, их преломление к познанию общества играют важную методологическую роль в расширении социально-философского знания феномена информационной безопасности.

2.3. ПРИНЦИПЫ ИНФОРМАЦИОННОЙ ЭТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЩЕСТВА И ЧЕЛОВЕКА

В самом широком смысле под словосочетанием «информационная этика» подразумевается ветвь прикладной этики, которая изучает и анализирует социальное и этическое влияние информационно-компьютерных технологий на все сферы общественной жизни. Согласно методологическому принципу антиномичности, в прикладной этике практические проблемы преломляются через дилеммы[1], то есть ситуацию выбора между взаимоисключающими нравственными решениями. В. Н. Назаров выделяет в области информационной этики наиболее животрепещущие моральные дилеммы, в число которых входит и информационная безопасность. В данном контексте моральные дилеммы отнюдь не безнадежны, они требуют духовно-нравственного пути разрешения сложной проблемы. По предположению специалистов, именно в области информационной безопасности потенциал информаци-

[1] Назаров В. Н. Прикладная этика. М. : Гардарики. 2005. С. 11.

онной этики нельзя недооценивать, поскольку это ее поле ответственности[1].

Именно информационная этика «максимально полно соответствует объективной реальности и учитывает специфику бытия человека XXI века»[2], потому в условиях постоянного роста информационной технологии теория информационной этики способна переосмыслить проблемы информационной безопасности и предложить духовно-нравственные рамки решения актуальных вопросов безопасности современного общества. В нашем случае новая этика информационного общества призвана дать философское осмысление основных проблем информационной безопасности и создать нравственное содержание деятельности по ее обеспечению, поскольку лишь одухотворенная деятельность может быть целесообразной и произвольной. На этом пути информационной этике, прежде всего как философской дисциплине, необходимо определить свои принципы.

По определению С. А. Радионовой под принципом понимается основание некой совокупности знаний, фактов, начальный пункт объяснения или исходное руководство к действию[3]. В философии принцип обусловливает начало всего существующего, закон становления явлений. Этот главнейший закон, истина, движущая сила, обладает внутренним единством и лежит в основе других законов или истин. В этике принцип связывают с внутренним убеждением, максимой, определяющей установку к действительности, всеобщую или частную норму поведения. На наш взгляд, в информационной этике принципы представляют внутреннюю

[1] Филина О. А. Социальные, культурно-исторические и ценностные основания информационной этики // Научные ведомости Белгородского государственного университета. 2009. № 9. Т. 10. С. 233.

[2] Коваль Е. В. Этика современного общества как современный этап развития этики // Вестн. Чуваш. ун-та. 2009. № 4. С. 134.

[3] Новейший философский словарь. Минск: Изд-во В. М. Скакун. 1998. С. 544.

убежденность и заданные нормы поведения, они регулируют поведение социальных субъектов в информационной среде, воплощая руководящее правило, инструментальное основание для той или иной деятельности в процессе информационных отношений.

Информационная этика занимается исследованиями в области фундаментальных понятий информационной безопасности: конфиденциальности, целостности и доступности информации, а также решением других актуальных вопросов в данной сфере, таких как профессиональная ответственность специалиста, интеллектуальная собственность и т. д. Несмотря на тот факт, что урегулирование поднятых вопросов, как принято считать, находится в большей степени в рамках законодательства государственных органов и технических решений, информационная этика предлагает собственные пути формирования универсальных оснований для определения справедливости и общего морального блага[1].

Основную задачу новой этики информационного общества Дж. Мур видит в анализе социального влияния компьютерной технологии и соответствующего формирования стратегии руководства действий человека в целях этического применения такой технологии. В свою очередь, выделяя актуальные проблемы информационной этики в области безопасности, Р. Капурро определяет этические принципы, призванные внести вклад в решение указанных проблем: принцип доступности и принцип полноты[2]. С нашей точки зрения, представленные принципы требуют большей конкрети-

[1] Warren S., Brandeis L. Privacy, photography, and the press // Harvard Law Review. Cambridge. 1891. Vol. 4; Gavison R. Privacy and the Limits of the Law // The Yale Law Journal. 1984. Vol. 8; Latak A. Identity Crisis: To make its players safe the NFL is tackling schemers and scammers. Legal Affairs // Retrieved. 2005. February [Электронный ресурс]. – URL: http://www.legalaffairs.org (дата обращения: 16.03.2014); Spinello R. Cyberethics: Morality and Law in Cyberspace, Third Edition. Sudbury. – Sudbury, Massachusetts: Jones and Bartlett Publishers, 2006.

[2] Capurro R. Information ethics // CSI-communication. 2005. Vol. 28. № 12.

зации и дополнения, кроме того, мы убеждены, в их число важно включить принцип конфиденциальности и принцип ответственности. Сформулируем основные принципы информационной этики в области обеспечения безопасности общества и человека.

Принцип доступности конкретизируется на преодолении политического, экономического и других видов ограничений с целью обеспечения максимального уровня доступности информации для каждого члена информационного сообщества. Этому принципу придается «высокое этическое значение»[1], поскольку он отвечает за урегулирование конфликтов информационного расслоения общества, информационного колониализма, проблемы этнических меньшинств и различного вида дискриминации.

На наш взгляд, приоритетные направления указанного принципа необходимо дополнить – внести в их число решение вопросов монополий и демократического управления в информационной среде современного общества. Указанная необходимость обусловлена, прежде всего, проблемой определения прав на интеллектуальную собственность в информационном мире, которая является одним из актуальнейших вопросов информационной безопасности. Нюансы определения границ данного понятия вызывают большое количество споров, сегодня концепция интеллектуальной собственности породила множество столкновений в мире компьютерной и киберэтики. С нашей точки зрения, это обстоятельство связано, прежде всего, с тем, что философия взаимодействия в сети Интернет сосредоточена вокруг свободы информации, от того и возникает существующая неоднозначность в отношении определения прав собственников интеллектуальной продукции.

[1] Capurro R. Moral issues in information science // Journal of information science. 1985. № 11. P. 116.

Передадим общие черты рассматриваемой проблемы. Постоянно растущая скорость передачи информации и появление технологий сжатия объемов информационного содержания открыли двери в мир мгновенного и анонимного обмена информацией, что, в свою очередь, породило постоянно растущее количество социальных, этических, правовых вопросов в отношении незаконной передачи контента, защищенного авторским правом. Два противоположных мнения сконцентрировано в споре о распространении закрытых программных продуктов и программного обеспечения с открытым исходным кодом. Аналогичные дебаты в области прав на интеллектуальную собственность протекают и в отношении файлов формата видео, музыкального и художественного содержания.

Сторонники наложения ограничений на совместное использование подобной информации аргументировано защищают собственные права, ссылаясь на отсутствие стимула компаний вкладывать ресурсы в развитие без должного объема доходов от продаж и лицензионных сборов. Здесь можно привести следующие доводы в защиту прав собственности: каков интерес компаний, вкладывающих значительные средства в разработку программного обеспечения, и программистов, работающих недели и месяцы над созданием компьютерных программ, если не в получении прибыли от вложений в форме лицензионной платы и продаж. В наше время индустрия программного обеспечения – это многомиллиардная долларовая часть экономики, компании по разработке программного обеспечения заявляют, что потери из-за нелегального копирования («пиратства») ежегодно составляют миллионы долларов. Индустрия программного обеспечения утверждает, что миллионы долларов в объеме продаж теря-

ются даже из-за «редкого копирования собственных программ для друга»[1].

В свою очередь, теория информационной этики в поиске решений проблемы определения прав на интеллектуальную собственность пытается выйти дальше рамок экономических составляющих вопроса. Так, особо подчеркивая проблему интернационализации сети Интернет, Т. Фрелих говорит о том, что в сложившейся ситуации обществу необходимо найти ответ на ряд сложноразрешимых вопросов. Является ли информация (контент и/или программное обеспечение) объектом интеллектуальной собственности? Насколько понятие «обмен знаниями» становится доминирующим над понятием «собственность»? Можно ли в условиях современного общества гарантировать равный доступ к информации?[2]

Данной точки зрения придерживается Дж. Мур, который так же озадачен решением проблемы определения интеллектуальной собственности в информационном мире. В рамках анализа «концептуальных путаниц»[3] он ставит следующие вопросы: насколько понятие «компьютерная программа» попадает под определение интеллектуальной собственности? Что это – объект, имеющий правообладателя, или идея, алгоритм без права владения? Если компьютерная программа все же объект интеллектуальной собственности, является ли она выражением идеи какого-либо владельца (традиционно охраняемой авторским правом) или это процесс, принадлежащий кому-либо (традиционно охраняемый патентом)? Является ли машиночитаемая программа копией языка программирования? На наш взгляд, заданное исследователями направление решения вопроса определения границ интеллек-

[1] Bynum T. The Foundation of Computer Ethics // Computers and Society. 2000. № 30(2). P. 12.
[2] Froehlich T. J. Ethical considerations of information professionals // Annual Review of Information Science and Technology. 1992. № 27.
[3] Moor J. What Is Computer Ethics? // Metaphilosophy. 1985. № 16 (4).

туальной собственности является верным, так как только концептуализация природы компьютерной программы, как и любого другого информационного объекта, поможет ответить на перечисленные вопросы и сформулировать нужную стратегию его защиты.

Весьма интересна точка зрения Р. Столмэна относительно проблем связанных с интеллектуальной собственностью. Он утверждает, что программное обеспечение не должно быть обременено чьим-либо правом. По его предположению, всякая имеющаяся информация должна быть свободной, все существующие компьютерные программы должны быть доступными для копирования, изучения и изменения для всех желающих. На наш взгляд, мнение ученого открыто отражает идеи философии сообщества хакеров[1], к сожалению, которые в настоящее время нашли только осуждение в обществе, а их деятельность преследуется законом. В тоже время, мы обязаны отметить, что в недрах современного общества зреют новые революционные взгляды относительно вопросов интеллектуальной собственности и авторского права. В силу того, что за последние 20 лет права интеллектуальной собственности разрослись «до масштабов монополии», демократически настроенное информационное сообщество видит необходимым пересмотреть подобные меры поощрения творчества относительно интересов современного общества в целом, не замыкаясь только на экономических интересах культурной сферы[2].

Взгляды Р. Столмэна находят поддержку в теории К. Химма, который также не может найти моральное оправдание существованию законного права исключать возможность

[1] Levi S. Hackers: Heroes of the computer revolution. – Harmondsworth United Kingdom: Penguin. 1983. P. 337.

[2] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный центр библиотечного сотрудничества. 2009.

доступа других к содержанию своих творений. В философских спорах об обосновании интеллектуальной собственности автор ставит под сомнение действия государства, предоставляющие право на охрану интеллектуальной собственности. К. Химма анализирует сложные вопросы данной области и внимательно изучает аргументы всех сторон дебатов. Он выявляет особый социальный характер интеллектуального содержания понятий «свободный доступ к информации», «информационные фонды» и «свобода слова»[1]. В попытке сбалансировать интересы спорящих сторон автор возвращается к классической теории Д. Локка о естественном моральном праве человека защищать свою собственность, теперь выраженную в информационных объектах, при этом не упуская из поля зрения такие аргументы, как затраченное время и труд. В результате К. Химма приходит к следующему выводу: законная защита интересов авторов – вопрос политической морали, защита содержания любого интеллектуального объекта в качестве собственности не всегда морально оправдана. Государство в принятии решения об ограничениях в использовании должно рассматривать в отдельности каждый конкретный пример, претендующий на право быть объектом интеллектуальной собственности. На наш взгляд, в складывающейся ситуации, когда информационные технологии трансформируют ценности и приоритеты, сформировавшиеся в индустриальном обществе, информационное общество меняет и привычные представления о праве собственности.

Т. Карбо и М. Смит видят свой путь решения поставленных вопросов. Они предлагают оригинальный «принцип рас-

[1] Himma K. Ethical Issues Involving Computer Security: Hacking, Hacktivism and Counterhacking. The handbook of information and computer ethics. Ed.: Himma K. and Tavani H. New Jersey: Wiley-Interscience. 2008.

пределенной этики»[1], в основе которого лежат нормативные требования относительно морального регулирования человеческого поведения. Максимальное число пользователей информационной системы, обладающих определенными возможностями, образуют распределенную многоагентную систему, характеризующуюся отсутствием централизованного регулирования. Подобная среда за счет реализации этических стратегий по обеспечению безопасности находится в особом «экологическом измерении» и как результат предоставляет программное обеспечение с открытым исходным кодом. При этом авторы идеи утверждают, что проблемы в компьютерной этике возникают из политического вакуума относительно использования новой технологии, что стандартных законодательных норм недостаточно для решения «технологических» проблем. На наш взгляд, Т. Карбо и М. Смит совершенно правы в своем предположении, что на данном этапе развития современного общества этические принципы, заложенные в основе саморегулирования человека, обеспечат некоторый порядок и послужат перспективным направлением будущих исследований.

В свою очередь, мы предполагаем, что право собственности на программное обеспечение – достаточно сложный вопрос, который возможно рассматривать с точки зрения разных аспектов: авторское право, профессиональная тайна и патенты. Обратим внимание на следующую специфику изучаемого вопроса. Готовая программа содержит несколько составляющих, в свою очередь, облагаемых правом собственности: «Исходный код» – высокоуровневый компьютерный язык; «Объектный код» – машинный кодовый перевод исходного кода; «Алгоритм» – последовательность ко-

[1] Carbo T., Smith M. Global information ethics: Intercultural perspectives on past and future research // Journal of the American Society for Information Science and Technology. 2008. № 59(7). P. 1110.

манд управления, представленная исходным и объектным кодом; «Впечатление и ощущение» от программы – интерфейс программы, от которого зависит ее степень взаимодействия с пользователем. В результате чего выдача патента на компьютерный алгоритм – еще одна трудноразрешимая задача в деле распределения прав собственности на программное обеспечение.

Как правило, обладатель патента имеет эксклюзивную монополию на использование зарегистрированного предмета или объекта, так что владелец алгоритма вправе отказать всякому, желающему использовать математические формулы, составляющие часть алгоритма. В данном случае математики возмущенно заявляют, что практика выдачи патентов на алгоритмы программ ведет к искоренению достижений математической науки из категории всеобщего достояния[1] и, как следствие, угрожает снижению общего потенциала будущих научных исследований. Стоит отметить, что на предварительные «поиски патента» с целью удостовериться, что в действительности созданная «новая» программа не нарушает ничьих авторских прав, требуется большое количество времени и средств. На практике подобная процедура доступна лишь крупным кампаниям, обладающим внушительными бюджетными капиталами. Мы убеждены, что описанная ситуация в конечном итоге устранит небольшие компании с рынка производства программных продуктов, чем создаст условия для развития монополий, подавляя конкуренцию и уменьшая разнообразие, благотворное для общества.

Действительно, поскольку компьютерная технология предоставляет новые возможности для действий, появляются новые ценности. Создание программного обеспечения, несомненно, имеет определенную ценность в культуре сего-

[1] Bynum T. The Foundation of Computer Ethics // Computers and Society. 2000. – № 30(2). P. 12.

дняшнего дня, о существовании которой несколько десятилетий назад никто не имел понятия, соответственно, некоторые ценности «прошлого» века требуют своего пересмотра. В итоге, информационная этика занимается исследованием альтернативных стратегий в области определения прав на интеллектуальную собственность в информационном мире, в результате чего вынуждает общество выявлять ценностные предпочтения.

Таким образом, принцип доступности конкретизируется на обеспечении максимального уровня доступности информации для каждого члена информационного сообщества, отвечая за урегулирование вопросов монополий и демократического управления в информационной среде.

Следующий принцип – принцип полноты, который указывает на необходимость решения вопросов информационного шума, он дает оценку содержанию информации, сосредоточенной в мировых информационных системах и сетях. В данном ключе автор видит необходимым завести речь об этической ответственности за достоверность и объективность размещаемой информации, в борьбе не за количество, а за качество ресурсов[1]. В свою очередь, мы считаем, что в рамках данного принципа помимо оценки полноты содержания информации необходимо обеспечить целостность информационного содержания в информационных системах и мировых информационных сетях.

Защита целостности информации на сегодняшний день является актуальнейшей проблемой в области информационной безопасности, основную угрозу которой представляют действия хакеров. Функции данной категории профессионалов и пользователей информационных технологий сводятся к созданию вредоносных программ и незаконному проникновению в чужую компьютерную систему, приводя тем самым

[1] Capurro R. Information ethics // CSI-communication. 2005. Vol. 28. № 12.

к нарушению целостности ее информационных ресурсов. При этом обычно по характеру вторжения в компьютерные системы хакеров делят на тех, которые намеренным образом совершают вандализм и похищают какие-либо данные, и тех, кто, руководствуясь исключительно интересом, просто «исследует» систему. Такие «исследователи» часто заявляют о себе как о благожелательных защитниках свободы и борцах против мошенничества в крупных корпорациях или шпионажа правительственных агентов. Эти самоназванные члены «комитета бдительности» кибернетики говорят, что они не причиняют вреда, и заявляют, что приносят помощь обществу, проявляя неблагонадежные элементы. Но, так или иначе, на наш взгляд, всякое действие хакера неизбежно наносит ущерб, поскольку требует от владельца компьютерной системы тщательной проверки на повреждения, потерю данных или программ. Даже в том случае, если хакер не произвел никаких изменений в информационной системе, владелец компьютера вынужден осуществить трудоемкий осмотр компьютерной системы.

Подобную току зрения поддерживает К. Химма, который к кибератакам причисляет нарушения целостности информации как без преступного умысла, например, из-за развлечения или любопытства, так и из-за желания завладеть незаконным путем конфиденциальной информацией в целях вымогательства, финансового обогащения, личной выгоды или намерения дезорганизовать работу информационной системы[1]. К одному из достоинств исследования К. Химма, на наш взгляд, стоит отнести его внимательное изучение этических проблем каждой из сторон киберконфликта. Он подробно рассматривает философию поведения хакера и этические

[1] Himma K. Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking. The handbook of information and computer ethics (eds.). Himma K. and Tavani H. New Jersey: Wiley-Interscience. 2008.

принципы, лежащие в основе его действий, взвешивает все за и против цифрового вторжения.

Сегодня равенство и демократия стали, возможно, спонтанно, но определяющими характеристиками сети Интернет, задающими новое, свободно организованное политическое измерение. Подобное либеральное выражение равенства утверждает равные возможности в электронной реальности независимо от этнической принадлежности, физических возможностей организма, пола, религии и т. д. Философия хакеров отличается яркими либеральными принципами, отражающимися в этических постулатах, определяющих поведение данной социальной группы. Кроме того, существуют конкретные случаи участия хакерского сообщества в законодательных процессах, оказавшие действительно решающее значение в дебатах о свободе слова и цензуре в среде Интернет[1]. Справедливо также отметить уникальную специфику сети Интернет, которая оказала революционное влияние на содержание таких понятий, как работа и досуг. Интернет положил начало новому подходу к работе, ломая привычное восприятие времени. Использование новой технологии позволяет изменять границы работы и отдыха в информационном обществе, в результате чего хакерскую этику причисляют к новой трудовой этике[2].

В то же время, отмечая возможные положительные социальные эффекты от «доброкачественного вторжения» хакеров, проливающего свет на уязвимые места систем защиты, необходимо подчеркнуть, что цифровое вторжение, даже не нарушая физическое пространство человека, несет потерю конфиденциальности информации, соответственно, морально оправдано быть не может. Что же касается роли государ-

[1] Taylor P. Hackers: Crime in the Digital Sublime. L., N. Y.: Routledge, 1999.
[2] Himanen P. The Hacker Ethic and the Spirit of the Information. Cambridge MA, London Age: MIT Press. 2001; Weber M. The Protestant Ethic and the Spirit of Capitalism. – London: Routledge. 1930.

ства, то в данный момент правоохранительные органы не имеют необходимых ресурсов для обеспечения минимальной защиты от действий хакеров, отчего решение проблем от цифровых нападений всецело ложится на плечи собственников информации. Так, в рамках теории информационной этики К. Химмой введено новое понятие «этика киберзащиты», служащее моральным оправданием действий последних в процессе защиты собственных информационных ресурсов.

С нашей точки зрения, здесь необходимо выделить важную мысль: исследования теории информационной этики не ставят цель дать четкие ответы на вопросы поставленной проблемы, но предлагают этические рамки, в которых возможно найти ее решение. Разработки в области информационной этики позволяют еще раз осмыслить спектр новых возможностей, ставших доступными человеку благодаря развитию информационных технологий, определить адекватное к ним отношение. Они задают моральные ориентиры человеческой деятельности в информационной среде, отвечающие инвариантным духовным ценностям и нравственным принципам поведения. В своих исследованиях философы иллюстрируют механизмы реализации принципа защиты целостности информации, позволяющего урегулировать вопросы безопасности. На наш взгляд, они совершенно правы в убеждении, что окончательное этическое решение в данном вопросе требует более тщательного анализа характера поведения каждого субъекта и контекста, в котором проводится конкретная кибератака.

Так, в рамках информационной этики рассматривается гендерное направление изучения вопросов компьютерной преступности. В противовес многим концепциям о торжествующем равноправии в информационной среде данное направление исследует вопросы о роли гендерных характеристик в процессе обеспечения безопасности и решения проблем этического использования информационной техноло-

гии. Киберфеминизм вырабатывает собственные подходы в изучении этических проблем, возникающих в процессе использования технологий современного общества. Под киберфеминизмом сегодня понимается направление в современной литературной и философской мысли в рамках феминистского дискурса, которое обратилось к изучению и популяризации основных принципов киберкультуры, сложившейся в 1980-е годы на Западе на волне интереса к феномену высоких технологий, прежде всего кибернетики, биомедицины и технологий виртуальной реальности[1].

Основные направления киберфеминизма относятся к социально-философским исследованиям информационной технологии и роли женщины в процессе ее применения. Целью исследований данной теории является борьба с традиционными представлениями о мужском контроле технологии, в частности новых информационных технологий, о достижении равенства женщин и мужчин в отношении их использования, то есть своего рода «некритический энтузиазм в области науки, техники и прав женщин»[2]. При этом сторонники указанного подхода ставят задачи выйти за пределы одного феминистского желания – подорвать мужской контроль управления информационными технологиями, но решить моральные, социальные, политические и правовые проблемы. В границах информационной этики киберфеминизм пытается найти ответ на вопрос о роли гендерного фактора на развитие киберпреступности.

Как правило, количество специалистов, занятых в области информационных технологий, неоспоримо ведет к преобладающему числу профессионалов среди мужчин, статистика расследования преступлений в информационной среде

[1] Словарь гендерных терминов [Электронный ресурс]. – URL: http://www.owl.ru/gender/096.htm (дата обращения: 26.03.2014).

[2] Stabile C. Feminism and the Technological Fix. – Manchester, N.Y. : University Press Manchester. 1994.

отражает преобладающее число хакеров мужского пола[1]. Относительно неуловимых женщин-хакеров выдвинуто несколько предположений. П. Тейлор связывает низкое число хакеров-женщин на фоне общего количества киберпреступников с параллельно низким числом женщин, занятых в области информационных технологий[2].

Другая группа ученых, основываясь на философии полов, объясняет данное явление следующим образом. В отличие от мужчин женщины более консервативны в своих этических суждениях, в результате чего по отношению к ним применение этических мер безопасности на уровне внушения будет достаточным, в то время как мужчины могут потребовать более существенных сдерживающих механизмов, регулирующих поведение в информационной среде[3]. Д. Мак-Махон и Р. Коэн отмечают явную связь пола с принятием этических решений в виртуальном онлайновом мире[4]. Согласно результатам их исследования, женщины чаще задумываются об этичности поступков, нежели мужчины.

Основатель теории хакерской этики С. Леви высказывает свое мнение по поводу рассматриваемой ситуации: «Нет мужского или женского хактивизма. Хакеров характеризуют результаты их деятельности, а не принадлежность к определенной расе, религии или полу»[5]. Он дает следующее описание поведению хакеров: «со стороны кажется, что хакеры ведут странные разговоры, у них нестандартный распорядок дня, они едят странную пищу, и они все свое время думают о

[1] Adam A. The Gender Agenda in Computer Ethics. Ed. Kenneth E. Himma and H. T. Tavani. N. Y. : John Wiley. 2008.
[2] Taylor P. Hackers: Crime in the Digital Sublime. – L., N. Y. : Routledge. 1999.
[3] Kreie J., Cronan, T. How men and women view ethics // Communications of the ACM. 1998. № 41(9).
[4] McMahon J., Cohen R. Lost in cyberspace: ethical decision making in the online environment // Ethics and Information technology. 2009. Vol. 11(1).
[5] Levy S. Hackers. Heroes of the Computer Revolution. Harmondsworth UK: Penguin. 1984. P. 378.

компьютерах»[1]. Анализируя признаки зависимости от интернет-сеансов, автор заключает: личные проблемы, связанные с гигиеной, женщины переносят сложнее, нежели мужчины, что уже может быть основанием для меньшего числа хакеров среди женщин.

В свою очередь, А. Адам и Е. Грин предполагают, что биологические и социальные функции, заложенные в женщине, изначально исключают ее из сообщества хакеров[2]. Действительно, в силу присущей ей обязанности заботиться о детях и доме женское представление о работе и досуге существенно отличается от мужского. Подобного взгляда придерживается А. Куд: «Трудясь в две смены – на оплачиваемой работе и дома»[3], женщина меньше всего готова посвятить ночное время хакерской деятельности, кроме того, компьютер не способен воссоздать работу по уходу за ребенком и семьей в реальной жизни. Мнение авторов таково, что коммуникационные технологии и сеть Интернет воспроизводят стандартные гендерные модели, предполагающие наличие свободного времени.

На наш взгляд, в сложившейся ситуации, прежде всего, необходимо выделить положительные аспекты идеи киберфеминизма, открывающие новый взгляд на решения этических проблем современного общества. Важно отметить, что социальные и политические позиции женщин, поддерживающих идеи киберфеминизма, предлагают альтернативные с этической позиции взгляды на хакерскую активность.

В данном ключе К. Соллфранк верно заводит разговор об особенностях женской хакерской этики, которая отличается

[1] Levy S. Hackers. Heroes of the Computer Revolution. Harmondsworth UK: Penguin. 1984. P. 173.

[2] Adam A., Green E. On-line leisure: gender and ICTs in the home. Information // Communication and Society. 1998. № 1(3).

[3] Cudd A. Objectivity and ethno-feminist critiques of science. In: Ashman K. and Baringer P. (eds.), After the Science Wars. N. Y., L. : Routledge. 2001. P. 80.

от мужских подходов в хакерской деятельности, например, в отношении таких аспектов, как свобода слова, дискриминация, защита прав детей[1]. Справедливо заключение С. Сегана о том, что проявления альтернативного движения феминистской хакерской этики в защиту общепринятых нравственных идеалов идут вразрез с провозглашенными традиционными хакерскими принципами свободы слова в сети[2]. В качестве примера здесь можно привести «крестовый поход» против порнографии в Интернете[3], когда женщины-хакеры использовали свои навыки и умения, чтобы выследить деятельность сайтов, специализирующихся на детской порнографии с целью передать информацию в правоохранительные органы.

По нашему мнению, действия женщин-хакеров еще раз служат подтверждением известной истины о том, что лишь нравственное содержание деятельности придает ей смысл. Гендерный подход решения проблем защиты информации исследует общий вклад феминистской версии информационной этики в борьбу за права человека информационного века и защиту нравственных идеалов общества. Анализируя данный подход, необходимо отметить, что феминистская этика, отличающаяся особой практичностью, дает новую трактовку некоторых этических аспектов в области информационной безопасности.

Таким образом, в эру компьютерных вирусов и киберпреступности тема безопасности информации наиболее ярко

---

[1] Sollfrank C. Not every hacker is a woman [Электронный ресурс]. – URL: http:www.obn.org/reading_room/writings/html/notevery (дата обращения: 30.09.2004).

[2] Segan S. Female of the species; hacker women are few but strong [Электронный ресурс]. – URL: http://more.abcnews.go.com/sections/tech/dailynews (дата обращения: 03.01.2003).

[3] ACPO AntiChildPornogr [Электронный ресурс]. – URL: http://www.antichildporn.org (дата обращения: 25.05.20014).

проявляет себя в области информационной этики. На наш взгляд, принцип полноты и целостности информации указывает на необходимость решения вопросов обеспечения безопасности информации и качества ресурсов, сосредоточенных в мировых информационных системах и сетях.

Третий принцип, который мы выделяем – это принцип конфиденциальности. В течение прошлых десятилетий коммерциализация и стремительный рост сети Интернет, повышение «дружественности» интерфейсов и вычислительной мощности компьютеров, уменьшение расходов на приобретение и содержание компьютерных технологий привели к новым проблемам, касающимся защиты персональной информации. Необходимо отметить, что вопросам конфиденциальности информации в обществе уже давно присуща особая актуальность, порождающая новые темы для обсуждения.

Изобретение первых видеокамер стимулировало первые этические дебаты, которые сегодня активно генерирует интернет-среда. Еще в 1890 году С. Уоррен и Л. Брандес пытались определить понятие «конфиденциальность» с философской точки зрения. По их убеждению, Достоинство, Индивидуальность и Конфиденциальность личности являются основополагающими составляющими понятия «независимость» человека. Это «необходимая площадь жизни человека, которая находится полностью под его контролем, область, которая является свободной от вторжения извне. Лишение же неприкосновенности частной жизни может представлять опасность для здоровья человека»[1].

Спустя более 100 лет сеть Интернет и распространение личных данных через различные информационные системы вызвали то самое явление, которое потребовало нового раун-

[1] Warren S., Brandeis L. Privacy, photography, and the press // Harvard Law Review. Cambridge. 1891. Vol. 4. P. 111.

да этических дебатов относительно конфиденциальности информации о личности человека. Например, насколько надежна степень обеспечения конфиденциальности информации сегодня в среде Интернет: о состоянии медицинского здоровья, о политических убеждениях и интересах отдельных граждан? При этом остается бесспорным тот факт, что обеспечение секретности информации в информационных сетях поддерживает и сохраняет такие человеческие ценности, как безопасность, психологическое здоровье, самореализация и душевное спокойствие. В противном случае слабый уровень обеспечения защиты секретности и конфиденциальности различного рода информации содействует развитию преступной среды, открывая новые пути для экономических преступлений, торговли наркотиками, актам терроризма, вымогательству и т. д.

Многочисленные вопросы в сфере сохранения секретности информации, вызванные использованием информационных технологий, подвели исследователей из разных областей наук к переосмыслению концепции секретности. В середине 1960-х годов разработанная теория секретности «Контроль над персональной информацией» вызвала бурное обсуждение в среде философов и социологов. Дж. Мур и Г. Тавани утверждают, что контроль над персональной информацией недостаточен для установления защиты секретности информации, а «концепция самой секретности лучше всего определяется в условиях ограниченного доступа, нежели контроля»[1]. В свою очередь, Г. Ниссенбаум писала, что чувство секретности возникает даже в местах общего пользования. Действительно, адекватное определение секретности должно принимать во внимание понятие «публичной секретности»[2].

[1] Tavani H., Moor J. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies // Computers and Society. 2001. № 31(1).
[2] Nissenbaum H. The Meaning of Anonymity in an Information Age // The Information Society. 1999. № 15. P. 141.

Р. Гэвисон в своем исследовании вопросов конфиденциальности информации в современном обществе условно разделяет информацию о человеке, требующую ограничения доступа, на «три элемента: секретность, анонимность и одиночество. Анонимность относится к праву человека на защиту от нежелательного внимания. Одиночество относится к недостаточной физической близости человека к другим. Секретность относится к защите персональной информации от свободного распространения»[1]. Указанная идея, по нашему мнению, легко находит свое подтверждение в реальности. Например, проведение различного рода операций в информационных сетях или регистрация услуг посредством информационных систем чаще требует определенного количества информации личного характера. Этические правила ведения деловой практики требуют обеспечения защиты конфиденциальности информации о клиентах, которая может привести к потере секретности, «анонимности» и «одиночества». Информация о кредитной карте, номер социального страхования, указание в качестве кодового слова девичьей фамилии матери и т. д., адреса и номера телефонов, свободно собранные и находящиеся в общих базах, доступных в сети Интернет, – все это уже ведет к потере конфиденциальности. «Мошенничество или всякого рода действия, связанные с прямым или косвенным злоупотреблением использования частной информации, кража частной информации в сети Интернет – одни из самых быстрорастущих преступлений. Государственные архивы, поисковые системы и базы данных являются главными виновниками, способствующими подъему киберпреступности»[2], – заключает Э. Латак, рассуждая о кризисе идентичности.

[1] Gavison R. Privacy and the Limits of the Law // The Yale Law Journal. 1984. Vol. 8.
[2] Latak A. Identity Crisis: To make its players safe the NFL is tackling schemers and scammers [Электронный ресурс]. – URL: http://www.legalaffairs.org (дата обращения: 16.03.2014).

В борьбе с указанной проблемой Р. Спинелло советует исключить чувствительные уникальные идентификаторы из записей баз данных[1]. Действительно, хранилища данных используются сегодня для сбора и содержания больших объемов персональных данных и информации о потребительских сделках, данные средства могут сохранять большие объемы информации на неопределенный промежуток времени. При этом некоторые из ключевых программных архитектур упомянутых баз данных способствуют эрозии конфиденциальности, включающей различные виды программ-шпионов, а из-за своих внушительных объемов легко обнаружимы и не защищены от взломов. Сегодня не вызывает сомнений важность вопроса о повышении уровня защиты данных, поскольку отсутствие ответственности в обращении с личной информацией, размещенной на корпоративных веб-сайтах и сайтах социальных сетей, недопустимо.

А. Уэстин, подробно исследовавший теорию конфиденциальности, считает, что неприкосновенность частной жизни имеет особое значение для обеспечения свободы и демократии[2]. Л. Хенкин считает, что конфиденциальность – важная составляющая для автономии человеческой личности[3]. Дж. Мур и Д. ДеСев, описывая необходимость защиты конфиденциальности как одной из человеческих ценностей, используют метафору «щита». Например, Дж. Мур олицетворяет частную жизнь с «щитом, защищающим лицо человека от некоторых негативных аспектов общества, а в некоторых случаях и от других членов общества»[4]. Д. ДеСев утвержда-

[1] Spinello R. Cyberethics: Morality and Law in Cyberspace. – Sudbury, Massachusetts: Jones and Bartlett Publishers. 2006.
[2] Westin A. Privacy and Freedom. N. Y. : Atheneum Press. 1967.
[3] Henkin L. Privacy and autonomy // Columbia Law Review. 1974. Vol. 77.
[4] Moor J. Using genetic information while protecting the privacy of the soul. In: Tavani H. T. (Ed.). Ethics, Computing and Genomics. – Sudbury: Jones and Bartlett, 2006. P. 114.

ет, что конфиденциальность действует как щит, защищая человека от вторжений и давлений внешнего мира, обеспечивая свободу и независимость[1]. Р. Познер представляет неприкосновенность частной жизни в качестве «плаща», укрывающего человека[2]. В свою очередь, П. Риган утверждает, что частная жизнь, имеющая несколько степеней секретности, не только представляет ценность для личности, но и важна для общества в целом[3]. Со своей стороны отметим широкую социальную значимость частной жизни как общественное благо демократической системы, а ее обеспечение – как результат политических дебатов, связанный с обеспечением баланса между конкурирующими ценностями и интересами различных сторон.

На наш взгляд, представленные взгляды исследователей, изучающих этические и социальные проблемы в сфере безопасности, раскрывают нравственное содержание понятия конфиденциальности в области информационной безопасности и его роль в глобальном информационном обществе. Введение принципа конфиденциальности в рамках теории информационной этики направлено на защиту моральных ценностей в процессе информационного взаимодействия, а также обеспечение справедливого порядка в информационной среде.

Таким образом, принцип конфиденциальности направлен на урегулирование вопросов защиты персональных данных от утечки, потери секретности и модификации различными способами в процессе деятельности информационных провайдеров и производителей баз и банков данных в информационном сообществе.

---

[1] DeCew J. Privacy and policy for genetic research. In: Tavani H. T. (Ed.). Ethics, Computing and Genomics. – Sudbury: Jones and Bartlett, MA. 2006. P. 74.
[2] Posner R. An economic theory of privacy // Regulations. 1978. May-June. P. 22.
[3] Regan P. M. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill, North Carolina: University of North Carolina Press. 1995.

Четвертый принцип, который мы рассмотрим – это принцип ответственности. Вопросы профессиональной ответственности специалистов информационной безопасности являются темой для обсуждения уже достаточно длительный период времени в сфере информационной этики. В рамках этических аспектов профессиональной информационной среды рассматриваются такие проблемы, как выбор этически верного действия при выполнении профессиональных обязанностей, значимость человеческих ценностей и добродетелей в специфике профессиональных ситуаций, справедливость и профессиональные обязательства. Под профессионалами в области информационных технологий имеются в виду не только программисты, системные аналитики, системотехники, продавцы компьютерного оборудования. Сюда относятся пользователи продуктами информационной технологии – это служащие банков, конструкторы машин, работники народного образования, медицинские работники, экономисты, политики, представители СМИ и т. д.

Вопросы профессиональной ответственности специалистов, работающих с информационными технологиями, иначе – компьютерных профессионалов, изучает Д. Готтербан в рамках проблем информационной этики[1]. Он обеспокоен тем, что в области профессиональной этики недостаточно внимания уделено ценностям, регулирующим ежедневные виды деятельности компьютерных профессионалов. Под компьютерными профессионалами здесь подразумеваются все, кто вовлечен в создание и использование этих артефактов. Этические решения, реализованные в период развития подобных артефактов, имеют прямое отношение ко многим из вопросов в концепции информационной этики. Компьютерные профессионалы, обладающие уникальными знания-

[1] Gotterbarn D. Computer Ethics: Responsibility Regained // National Forum: The Phi Beta Kappa Journal. 1991. № 71.

ми, способны вносить преобразования в информационный мир, в результате чего внушают в сообществах особое уважение. Но «с подобной силой и возможностями приходят обязанности и ответственность»[1], – заключает Д. Готтербан. Мы можем заключить, что информационную этику следует рассматривать так же, как и профессиональную этику, направленную на развитие и продвижение стандартов хорошей практики и правил поведения для профессионалов, ведущих деятельность в информационной среде.

В свою очередь, Д. Джонсон пишет, что компьютерный профессионал, «занимаясь своим делом, вступает во взаимоотношения с работодателем, клиентом (или потребителем), с собратом по профессии и со всем сообществом»[2]. «У каждого из этих специалистов есть власть, и их решения способны влиять на общество в целом»[3]. Это означает, что компьютерные профессионалы получают власть над отдельными людьми, социальными институтами и даже над окружающей средой.

Исследователи совершенно правы в том, что компьютерный профессионал, как и любой другой профессионал, должен испытывать на себе действие категорического императива. В информационной практике достаточно часто возникают ситуации, в которых происходит столкновение чьих-либо интересов. Как правило, при более ответственном подходе компьютерные профессионалы пытаются сознательно избегать возможных конфликтов интересов всех сторон. Один чаще практикуемый путь решения описанной задачи заключается в принятии уставов организаций, этических кодексов, нормативов учебных программ и требований к аккредитации, регулирующих принципы профессиональной и

[1] Gotterbarn D. Informatics and Professional Responsibility // Science and Engineering Ethics. 2001. № 7(2). P. 221.
[2] Johnson D. G. Computer ethics. New Jersey: Prentice Hall. 1985. P. 26.
[3] Тоффлер Э. Метаморфозы власти. М. : АСТ. 2003. С.189.

этической ответственности в помощь компьютерным профессионалам.

Кроме того, необходимо отметить, что проблемы ответственности компьютерных профессионалов распространяются как на общество в целом, так и на отношения внутри профессиональной среды, которые непосредственно влияют на качество работы. В этой связи Р. Спинелло справедливо отмечает, что создание интеллектуального программного обеспечения привело к возникновению новых этических проблем[1]. Действительно, процесс создания экспертных систем включает деятельность как минимум двух категорий компьютерных профессионалов: доменный эксперт (domain expert) и инженер знания (knowledge engineer). Инженер знания – программист, ответственный за создание экспертной системы. Доменный эксперт отвечает за экспертизу в предметной области экспертной системы. Этические проблемы возникают в том случае, если нарушается взаимопонимание между обеими сторонами. Если инженер знания неправильно поймет доменного эксперта, то это непонимание может нарушить эту систему. Если решение экспертной системы окажется ложным, то ответственным за это могут быть и инженер знания, и доменный эксперт, и пользователь системы. Подобная ситуация выглядит трудноразрешимой, тем более что разные эксперты могут придерживаться противоположных точек зрения на решение одной и той же проблемы в зависимости от ее понимания. Врачи, юристы, экономисты и т. д. могут предлагать собственное видение той или иной проблемы, но программист обязан в задаче реализовать зачастую конфликтующие точки зрения.

В свою очередь, Дж. Мур в работе программного обеспечения выделяет три класса «невидимых» факторов, обла-

[1] Spinello R. A. Ethical aspects of information technology. New Jersey: Englewood Cliffs, 1995. P. XI.

дающих важным этическим значением[1]. Первый класс он назвал «невидимым обманом», обозначающим намеренное использование операций процессора с целью осуществить неэтичное, даже преступное действие. Например, программист, работающий в банке, в принципе может похитить так называемый «избыточный процент». В ходе банковских операций при подсчете процентов по вкладам после округления сумм обычно остаются доли цента. Программист может написать и ввести в компьютер программу, позволяющую переводить эти остаточные доли цента со всех банковских счетов и всех операций на свой счет, осуществляя тем самым похищение «избыточного процента».

Второй класс «невидимых» факторов – это «невидимый комплекс вычислений» программных технологий. Выполнение за доли секунд компьютерных расчетов, непостижимых для человеческого сознания, контроль над которыми неосуществим, рождают проблему доверия к «невидимым вычислениям».

К третьему классу «невидимых» факторов информационно-компьютерной технологии относится, в частности, присутствие «невидимых ценностей программы», то есть ценностей, вводимых в программу ненамеренно и до поры до времени неизвестных ни тем, кто пользуется программой, ни даже тем, кто ее составляет. Такую «невидимую ценность» иллюстрирует авария АЭС на Трехмильном острове США в 1979 году. Компьютер станции был запрограммирован моделировать возможные сбои и нарушения в работе АЭС, причем программа позволяла по последней логической цепочке вычислять, какие новые нарушения будут вытекать из случившейся ситуации. Однако авария произошла. В результате расследования было установлено: «моделирующее устройство не было запрограммировано для отладки одновременно

[1] Metaphilosophy. Oxford, 1985. Vol. 16. № 4. P. 273.

нескольких независимых нарушений»[1], что и послужило причиной аварии. Таким образом, неадекватность компьютерного моделирования оказалась результатом решения, принятого в процессе программирования. Во время аварии на Трехмильном острове операторы столкнулись именно с такой ситуацией.

На наш взгляд, описанная ситуация раскрывает еще одну важную проблему в области применения информационных технологий: насколько морально оправданно делегирование ответственности компьютерным системам? Передача информационным системам все большего числа функций управления и контроля во всех сферах деятельности, включая государственную оборону, усиливает опасность утраты человеком моральной, правовой и просто функциональной ответственности. Анализируя проблему моральной ответственности в условиях широкого применения информационных технологий, возникает вопрос, насколько освобождается человек от ответственности за ошибки программных средств и в каком смысле может быть ответственна сама информационная система? Какова персональная юридическая и моральная ответственность конструктора системы, разработчика программы, руководителя вычислительного центра, политика за ложные решения, подсказанные компьютером? Мы убеждены в том, что моральная ответственность – персональная или совместная – не может быть делегирована запрограммированным системам в качестве нормативного предписания, так как компьютер никогда не станет юридическим лицом, носителем морально-практического разума. В

[1] Галинская И. Л., Панченко А. И. Компьютерная этика, информационная этика, киберэтика (Этико-правовое пространство информационно-компьютерных технологий) // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. М. 2003. С. 132.

этой связи вопрос о «компьютерных ошибках» представляет особую этическую и правовую проблему.

В череде проблем относительно моральной ответственности неоднозначным выглядит и следующий вопрос: попадает ли распространение дефектной электронной информации под квалификацию «нарушение моральной ответственности»? Согласно законодательству, компании перед продажей обязаны тестировать свои продукты. Однако продукция, о которой идет речь, не похожа на машину или книгу. Например, в сфере медицинского знания экспертные системы ставят диагноз и предписывают лечение на основании описания симптомов болезни. Какой бы надежной ни была совершенная экспертная система, врач не может опираться только на ее выводы и рекомендации, он должен иметь собственное мнение. Если лечение окажется неэффективным, врач не может ссылаться на неисправность работы системы, поскольку она не несет ответственности перед законом и людьми. Кроме того, стоит учитывать «логическую податливость компьютера», то есть компьютер может быть запрограммирован для решения любой задачи независимо от ее этической ценности. Возможно, путь решения этого вопроса – в поиске способа придания информационным системам косвенной моральной релевантности. Важно отметить, что кое-где используется практика информационных систем, позволяющих осуществлять прямой или скрытый контроль над человеком. Во множестве случаев работа превращается в инструктаж компьютера.

В свою очередь, подробно исследуя вопросы профессиональной ответственности специалистов в области информационных технологий, Р. Шульц четко разграничивает смысл терминов «обязанности» и «обязательства»[1]. Первые выте-

[1] Schultz R. Contemporary issues in ethics and information technology. – Hershey: IRM Press (an imprint of Idea Group Inc.). 2006. P. 46.

кают с момента подписания трудового соглашения, в отличие от вторых, которые человек приобретает независимо от каких-либо договоров, здесь он употребляет понятие «долг». Задача этики заключается в поиске принципов, которые призваны решить противоречивые интересы «территорий» человека: гражданина, специалиста, отца (матери). Для достижения поставленной цели важно определить этические обязанности IT-специалистов: этические обязанности гражданина и личности; обязанности и обязательства как сотрудника в отношении работодателя; профессиональные обязанности по отношению к коллегам; основные обязанности по отношению к пользователям; основные профессиональные обязанности.

Каждая представленная категория, по нашему мнению, имеет различную этическую основу и статус, которые обязывают примерять человека различные роли. Если первая группа не несет в себе ничего специфического с точки зрения профессиональной этики, то следующие требуют от человека определенной степени ответственности, выражающейся в постоянном поддерживании статуса профессионала, грамотном использовании ресурсов и повышении уровня знаний, от которых зависит в конечном итоге качество работы. Необходимо отметить, что особая роль в выполнении поставленных задач принадлежит профессиональным этическим кодексам, которые призваны повысить качество работы, обеспечить сотрудничество коллег-профессионалов в направлении достижения профессиональных целей и донести до общественности идеалы профессии.

В результате анализа взглядов основных теоретиков концепции информационной этики нами отмечено, что новая прикладная область этического анализа исполняет особые функции в области морального регулирования профессиональной деятельности специалистов. В данном ключе информационная этика решает вопросы формирования нрав-

ственных образцов профессиональной деятельности, воспитания моральных принципов ответственности специалиста, выработки инструментов и механизмов этического саморегулирования и регулирования в профессиональной среде, связанной с использованием и созданием информационных технологий. В то же время современная информационная технология развивается неимоверными темпами, предлагая новейшие методы компиляции, хранения, доступа и анализа информации, стоит предположить, что философские дебаты о степени профессиональной ответственности специалистов далеки от завершения.

Так, в рамках изучения основных направлений принципа ответственности необходимо рассмотреть проблемы моральной ответственности специалистов, профессиональная деятельность которых основана на использовании новейших информационных технологий в области научных исследований человека.

Технократия упорно старается стереть границу между человеком и компьютером, между человеком и машиной. Д. Харавэй описывает состояние современного человека в качестве гибрида машины и живого организма. «Трансгрессия, нарушение границ между определением человеческого и машинного, начиная с очков, слуховых аппаратов, кардиостимуляторов, протезов, коронок, искусственных суставов, дополненное автоматизированной работой компьютеров и сетей, факсов, модемов, что в итоге превращает людей в киборгов»[1].

Изучая смысл человеческого существования в цифровом измерении, в качестве одной из главных задач информационной этики является забота о человеческом существовании. «Современные технологии, предоставляющие возможности

[1] Haraway D. Simians, Cyborgs and Women: The Reinvention of Nature. L. : Free Association Books. 1991. P. 150.

рассматривать человеческое тело как часть комплексной системы естественных и искусственных сообщений, которые функционируют на цифровой основе, то есть представляют его в качестве данных, имеют необратимые последствия в человеческом сознании и среде обитания человека. Описанная точка зрения несет в себе культурные изменения, поскольку исключает явления более высокого уровня, такие как человеческая психика и человеческий язык, или рассматривает их с позиции оцифровки, что неизбежно ведет к редукционизму, упрощению сложных связей между человеческим телом, языком и воображением»[1]. Так, нравственный императив несет уважение к телесному существованию человека в данном экзистенциональном смысле, проводя четкую границу между людьми с присущей им моралью, с одной стороны, и артефактами – с другой.

Н. Винер, основоположник кибернетики и величайший романтик машинной эпохи, обрисовал перспективы реализации идеи – симбиоза машины и человека[2]. Объединение живой плоти и неживой посредством локальной сети нашего организма, нервной системы, было для Винера в первую очередь попыткой помочь человеку обрести новые возможности или вернуть утерянные. Претворяя эту идею в жизнь, в 2001 году осуществили первое соединение нейрона с чипом[3]. Основная суть этого подхода – объединение сильных сторон человека и компьютера. Человек должен использовать интуицию, ассоциации и свое понимание процессов. Компьютер, в свою очередь, выполняет громоздкие точные расчеты и расширяет эффективный объем оперативной и долговремен-

[1] Ethical Aspects of ICT Implants in the Human Body [Электронный ресурс]. – URL: http://ec.europa.eu/european_group_ethics/avis/index_en.htm (дата обращения: 16.03.2005).

[2] Винер Н. Творец и робот. М. : Прогресс. 1964.

[3] Золотов Е. Рождение киборга [Электронный ресурс]. – URL: http://www.computerra.ru/online/firstpage/politica (дата обращения: 03.02.2014).

ной памяти человека. На протяжении нескольких десятилетий вычислительная мощность, обнаруживаемая в лучших образцах искусственного интеллекта и робототехнических систем, оставалась на уровне мощности мозга насекомых. Когда искусственный интеллект достигнет человеческого уровня, это даст еще более сильный толчок дальнейшему развитию. На наш взгляд, изучение моторных функций – не самое интересное, что обещает эксперимент: возможно, это путь к сложнейшим машинным интерфейсам будущего, наделению человека экстрасенсорными способностями, моменту, когда суперинтеллект, или чистый интеллект, окажется технически возможен.

С каждым шагом на пути к суперинтеллекту связаны громадные экономические выгоды. Компьютерная индустрия инвестирует огромные суммы в следующие поколения машин и программного обеспечения. Люди хотят иметь лучшие компьютеры и более умное программное обеспечение, получать выгоды, которые эти машины могут помочь производить. Лучшие лекарства, освобождение людей от необходимости выполнять скучные и опасные виды работы, развлечения – нет конца перечню выгод для потребителей. Существует также сильный военный мотив в разработке искусственного интеллекта. На этом пути какой-либо естественной точки остановки нет, где могли бы сказать «до сих пор, но не дальше».

Когда ставится вопрос об искусственном интеллекте человеческого уровня или выше, на пути дальнейшего развития могут оказаться политические силы. Суперинтеллект может рассматриваться как создающий угрозу превосходству и даже выживанию человеческого вида. Может ли человечество соответствующим программированием организовать мотивационную систему суперинтеллекта таким образом, чтобы гарантировать подчинение людям? Могут быть уверены политики будущего, что искусственный интеллект не подверг-

нет опасности интересы человека? Коллективное решение запретить новые исследования в этой области не может быть достигнуто и успешно воплощено – потому, что люди не будут рассматривать постепенное замещение биологических людей искусственно созданными машинами как нечто обязательно плохое. Может быть, из-за действия других мощных сил – мотивации краткосрочными прибылями, любопытства, идеологии, потребности в возможностях, которые суперинтеллект дает его создателям. «В течение ближайших тридцати лет у нас появится техническая возможность создать сверхчеловеческий интеллект. Вскоре после этого человеческая эпоха будет завершена»[1]. Если найдется способ гарантировать, что сверхчеловеческий искусственный интеллект будет подчиняться людям, то такой интеллект будет создан. Если нет возможности этого гарантировать, тем не менее, вероятно, он все равно будет создан.

Революционная ситуация в генетике вызывает философскую рефлексию по поводу ближайших и отдаленных последствий вмешательства в человеческий тип. До тех пор, пока речь шла об эффективности клонирования для обеспечения сфер жизнедеятельности человека – в рыбном хозяйстве, в сельском хозяйстве, растениеводстве, – проблема не обретала такую остроту. Вопрос о клонировании человеческого существа потребовал усилия многих теоретиков для осмыслений последствий такого шага.

Результаты исследований в области генной инженерии содержат в себе потенциальную угрозу для человека. Моральные проблемы, связанные с проектом генома человека, напоминают о том, что человек есть нечто большее, чем носитель генетических свойств. Человек, прежде всего, суще-

[1] Vindg V. The Coming Technological Singularity: How to Survive in the Post-Human Era [Электронный ресурс]. – URL: http://andrzej.virtualave/singulariti.html (дата обращения: 15.07.2012).

ство социальное, он является членом семьи, коллектива, нации и т. п. Разнообразие генетических признаков существует независимо от мечты о генетическом совершенстве. На наш взгляд, в данном случае необходимо сохранить баланс между благом отдельного индивида и благом сообщества. Что именно является «благом», лежит за пределами биологической науки. Биотехнология является продуктом творческих усилий многих, однако ее применение зависит от моральной ответственности человечества в целом. Человек в настоящее время способен изменить не только собственные гены, но и гены любого организма, но и, следовательно, экосистему всей планеты.

Исследуя эпистемологические и этические аспекты генетики, А. Мартурано приходит к выводу, что живой организм в каждый момент своей жизни является уникальным следствием истории своего развития, является результатом взаимодействия определенных внутренних (генетических) и внешних (экологических) сил, при этом такие внешние силы сами по себе являются частично следствием деятельности организма[1]. Относительно проблем генной инженерии и клонирования Л. Флориди приводит гипотетический пример. Если бы путем клонирования стало возможным вывести таких коров, которые бы не имели никаких нервных сенсорных волокон и, следовательно, не чувствовали боли, а только увеличивали массу тела при правильном кормлении, то их не нужно было бы убивать, чтобы получить мясо. Достаточно было бы вырезать у животного нужные части тела, не причиняя ему ни боли, ни страдания. Вопрос не в том, морально ли создавать таких чудовищ, а в том, как этика может оправдать обращение с ними. С точки зрения информационной этики

[1] Marturano A. Genetic Information: Epistemological and Ethical Issues. In Himma K., Tavani H. (Ed.) The handbook of information and computer ethics. New Jersey: Wiley-Interscience. 2008.

«бесчувственная корова» все равно является биологической массой, целостность которой требует уважения. Что же касается клонирования не ощущающих боли людских особей ради использования их органов, это морально недопустимо.

В памятниках мировой интеллектуальной мысли с легкостью обнаруживаются следы обсуждения данной проблемы задолго до ее постановки на волне научно-технического прогресса. Так, тексты Каббалы запрещают саму возможность помыслить о создании человека по заданным параметрам, за этим стоит космическое всевластие во многом нравственно несовершенного существа. Такой сверхчеловек устраняет саму идею Бога. Доктор Фауст Гете пытается создать искусственного человека – гомункулуса, и при этом присутствует сила зла – Мефистофель. Проблема сверхчеловека, поставленная Ф. Ницше, напрямую связана с выводом: «Бог умер!». Хаксли в романе «О дивный новый мир» описывает генетические манипуляции с эмбрионами. Наконец, идеологический заказ на евгенику, предполагающую вмешательство в природу человека, использование достижений генетики в целях государственной политики, формулирование идеи искусственного отбора в условиях ослабленного естественного, свидетельствует о вероломстве псевдонауки[1].

Все религиозные институты настаивают на том, что в формировании человека нужно стремиться к раскрытию образа и подобия Бога в нем, а не к созданию кощунственной пародии на его личность. Клонирование – это вызов религиозной морали, измена ее принципам. Согласно буддизму, генетически наследуемые черты не определяют всю природу человека. На их взгляд, нелепо было бы пытаться генетически сконструировать такие сложные человеческие качества, как моральная устойчивость, искренность и сострадание и т. п. В рамках этого учения стоит вопрос не о том, может ли

[1] Лешкевич Т. Г. Философия науки: Традиции и новации. М. : Приор. 2001. С. 18.

человек реконструировать душу и тело другого человека, а о том, нужно ли это делать. При анализе таких форм человеческой деятельности, как биоинженерия и клонирование, представителей буддизма интересуют, прежде всего, намерения и желания, лежащие в основе этой деятельности. С точки зрения буддизма эгоистические желания не могут лежать в основе благих поступков. Буддисты указывают на серьезный психологический риск, связанный не только с клонированием, но и любой технологией, которая сулит больший контроль над процессом воспроизводства, чем та, которой мы располагаем в настоящее время. Речь идет об уровне деспотического контроля над личностью[1], сконструированной в результате клонирования.

Мораторий на исследования в области генной инженерии, наложенный в 1974 году, является свидетельством возрастания тревоги прогрессивно настроенных ученых за судьбы социального применения научных достижений. Мораторий был снят только после острых дебатов относительно гарантий, исключающих их неугомонное использование или случайный вред. По мнению американского ученого П. Диксона, любой способ, который испробован на млекопитающих, может быть применен к людям. В этом случае общество попадет в ситуацию реальной множественности, в которой не отличить, где генетически подлинное существо, а где артефакт – искусственно созданное. Согласно публикациям[2], в 1998 году американский физик Р. Сид на симпозиуме по репродуктивной медицине заявил о намерении приступить к работам по клонированию человека вместе с группой медиков и лиц, стремящихся обрести копии или быть донорами. Исследования общественного мнения в США по этому во-

[1] Barnhart M. G. Nature, nurture and no-self: Bioengineering a. Buddist values // J. of Buddistethics. L. 2000. Vol. 7. № 3.

[2] Декларация в защиту клонирования и неприкосновенности научных исследований // Человек. М. 1998. № 3.

просу показали, что многие ученые недовольны стремлением официальных властей представить проблему «утечки» из лабораторий искусственно созданных микроорганизмов и заражения ими населения только как техническую проблему, оставляя в стороне философские, этические и политические аспекты[1].

Сегодня развертывается движение ученых за более действенный социально-этический контроль над научными исследованиями и их технологическим применением. Мы убеждены в том, что этическое регулирование науки становится новым этапом развития науки и актуальнейшим вопросом в рамках информационной этики. Ответственность и свобода научного поиска не являются альтернативными. В современных условиях этические проблемы возникают по отношению к науке в целом. Поэтому дискуссии по проблемам, связанным с регулированием исследований в области генной инженерии, нельзя рассматривать как нечто случайное для развития науки. Сознание этого все глубже проникает в современную науку и создает практические возможности для диалога и совместных действий внутри мирового научного сообщества[2].

У первых греческих мыслителей любовь к мудрости начиналась с этических принципов, вроде «меру во всем соблюдай», которые и сейчас вполне могли бы выступать в качестве регулятора человеческого поведения. Оценить долг и степень ответственности рационального индивида в терминах расширяющейся информационной сферы – главная задача информационной этики. В итоге процесс решения проблем информационной безопасности нуждается в постоян-

[1] Лазар М. Г. Этика науки: Философские аспекты соотношения науки и морали. Л. : Ленинград. ун-т. 1985. С. 75.

[2] Фролов И. Т. Избранные труды. Т. 2: Философия и история генетики. М. : Республика. 2002.

ном философском осмыслении и поиске ответов путем интроекции этических подходов.

На наш взгляд, все вышеизложенное демонстрирует факт постоянно расширяющегося поля деятельности информационной этики, еще раз утверждая необходимость принятия принципа ответственности, роль которого в плане обеспечения безопасности неизмеримо возрастает. Таким образом, принцип ответственности обязан задавать ценностные ориентиры и морально регулировать профессиональную деятельность специалистов в процессе применения информационных технологий.

Подведем итог. В области информационной безопасности информационная этика формулирует свои принципы, регулирующие общественную деятельность в информационной среде.

Принцип доступности конкретизируется на обеспечении максимального уровня доступности информации для каждого члена информационного общества, преодолении политического, экономического и других видов ограничений и дискриминации, отвечая за урегулирование вопросов монополий и демократического управления в информационной среде.

Принцип полноты и целостности информации указывает на необходимость решения вопросов обеспечения безопасности информации и качества ресурсов, сосредоточенных в мировых информационных системах и сетях.

Принцип конфиденциальности направлен на урегулирование вопросов защиты персональных данных от утечки, потери секретности и модификации различными способами в процессе деятельности информационных провайдеров и производителей баз и банков данных в информационном сообществе.

Принцип ответственности обязан задавать ценностные ориентиры и морально регулировать профессиональную дея-

тельность специалистов в процессе применения информационных технологий.

Основные принципы информационной этики, в целях достижения образцов справедливости, гуманизма, защиты моральных ценностей в процессе применения информационных технологий и социальных отношений в информационной среде позволяют создать нравственную основу для обеспечения деятельности современного общества в сфере информационной безопасности. Следующим шагом на этом пути является внимательное изучение социальных механизмов их популяризации и утверждения в сознании каждого субъекта и общества в целом.

ГЛАВА 3. РЕГУЛЯЦИЯ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА В ИНФОРМАЦИОННОЙ СРЕДЕ: ПРАВА И ОБЯЗАННОСТИ

3.1. ПРАВА ЧЕЛОВЕКА В КОНТЕКСТЕ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Результаты использования информационных технологий прямым образом зависят от рамок, в которых протекает заданный процесс. Дело в том, что он может быть ориентирован против идеалов гуманизма, в подобном случае масштабы последствий станут непредсказуемыми для всей человеческой цивилизации. Лишь гуманистическая направленность применения информационных технологий, изучение эффектов от их использования помогут создать благоприятные условия для безопасного формирования общемирового информационного пространства.

Принято считать, что технология сама по себе нейтральна, в прямом смысле она не может каким-либо образом оказывать негативное или позитивное влияние на развитие общества. В то же время пути использования возможностей, предоставляемых информационными технологиями, могут способствовать продвижению ценностей человека и его прав или быть диаметрально противоположными данной задаче. С ростом значения роли информационных технологий в повседневной жизни общества и человека растет понимание о необходимости регулирования процесса их развития и применения. Вопрос о том, как не допустить произвольное использование информационных технологий, но контролировать их развитие с учетом гуманистической направленности развития информационного общества, становится все более и более актуальным.

Гуманистическая направленность процесса использования информационных технологий, прогнозирование и контроль результатов их применения позволяет найти оптимальные решения проблем современного общества и человека. Масштабное приложение современных технологий не должно подчинять человека или уподоблять его компьютеру, подобная ситуация ведет к извращению изначальной цели создания технологии – облегчение труда и содействие творчеству человека.

Информационное общество должно стимулировать такое развитие и использование информационных технологий, при которых их преимущества будут оптимизированы, а отрицательное влияние сведено к минимуму[1]. На наш взгляд, в качестве базового приоритета будущего информационного общества необходимо рассматривать обеспечение прав человека и его фундаментальных свобод. В этой связи исследователи[2] предлагают ориентироваться на основные положения Всеобщей декларации прав человека[3], поскольку многие из них имеют особое значение для рассмотрения социальных и этических аспектов информационных технологий и возможных способов их использования.

И. Бриц верно указывает на то, что будущие перспективы глобальной информационной этики заключены в глобальной социальной справедливости информационного об-

---

[1] Этические аспекты новых технологий. Обзор. М. : Права человека. 2007. С. 17.

[2] Britz J. Making the global information society good: A social justice perspective on the ethical dimensions of the global information society // Journal of the American Society for Information Science and Technology. 2008. Vol. 59(7); Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract no. 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur, 1997; Капурро Р. Информационная этика // Информационное общество. 2010. Вып. 5. С.11.

[3] Всеобщая декларация прав человека [Электронный ресурс]. – URL: http://www.un.org/ru/documents/decl_conv/declarations (дата обращения: 22.01.2014).

щества. Обсуждая социальную справедливость в качестве нравственной нормы, которую необходимо использовать для решения этических проблем, стоящих перед современным обществом, И. Бриц цитирует Декларацию прав человека ООН, выделяя узловые аспекты из ее положений: отстаивать основные права и фундаментальные свободы человека; предупреждать негативные эффекты от использования современных информационно-коммуникационных технологий[1]. Т. Фрелих предполагает, что в основе процесса обеспечения безопасного использования информационных технологий заложена защита прав человека. При этом моральная ответственность за не нарушение перечисленных принципов распространяется на микроуровне (индивидуальном), мезоуровне (коллективном) и макроуровне (общественном)[2]. На наш взгляд, указанные мнения весьма точно определяют направление процесса информационной безопасности и развития общества в целом.

Понятие «право» подразумевает определенную ценность и меру свободы индивида, оно имеет прямую связь с моралью и призвано регулировать его поведение. Кроме того, данное понятие представляет собой инструмент социальной регуляции, обеспечивающий человека свободным выбором цели и деятельности, гарантирующий ему защиту[3]. Особым значением в этой связи обладают моральные права человека. В свое время различные философские концепции сложили классическое представление о естественных правах человека. Так, для Г. Спенсера – это жизнь, свобода, безопасность[4].

[1] Britz J. Making the global information society good: A social justice perspective on the ethical dimensions of the global information society // Journal of the American Society for Information Science and Technology. 2008. Vol. 59(7).
[2] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract no. 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur, 1997.
[3] Петрунин Ю. Ю., Борисов В. К. Этика бизнеса. М. : Дело, 2000. С. 78.
[4] Спенсер Г. Социальная статика. Киев: Гама-Принт. 2013. С. 111.

Точка зрения Дж. Локка характеризует права человека, заменяя «безопасность» на «собственность»[1]. Американская Декларация независимости Т. Джефферсона исключает «собственность» из данного списка, внося в него «право на счастье»[2]. Французская Декларация 1979 года в качестве главных ценностей предлагает свободу, собственность, безопасность и сопротивление угнетению[3]. В свою очередь, И. Кант полагает, что единственным правом человека остается только «свобода»[4]. Но независимо от интерпретации, именно имманентные нравственные ценности формируют основы этических правил. Сегодня, в период глобализации, общество формулирует свои нравственные ориентиры.

Выделим и рассмотрим основные положения пунктов Декларации прав человека ООН, представляющие особое значение с точки зрения информационной безопасности. По нашему мнению, статьи Всеобщей декларации прав человека отражают следующие принципы информационной этики в области безопасности: соблюдение конфиденциальности информации (ст. 1, 2, 3, 6, 12); принцип доступности, обеспечивающий равенство возможностей (ст. 2, 7, 18, 19, 20, 26, 27); принцип полноты и целостности информации (ст. 12, 19, 21); принцип ответственности (ст. 12, 19, 21).

Исключение различного рода дискриминации на пути достижения всеобщего и равного доступа к информации и информационно-коммуникационным технологиям утверждает статья 2 и отдельные положения статьи 7. Информационные технологии, непрерывно накапливая и анализируя информацию, формируют несчетное количество банков данных классифицируемой информации, в которых персональные

[1] Локк Дж. Сочинения: в 3 т. М. : Мысль. 1988. Т. 3. С. 269-270, 310.
[2] США. Конституция и права граждан. М. : Мысль. 1987.
[3] Французская Республика: Конституция и законодательные акты. М. : Прогресс. 1989.
[4] Кант И. Сочинения: в 8 т. М. : Чоро. 1994. Т. 3. С. 584.

данные делятся на следующие категории: пол, этническая принадлежность, социальный статус, исповедуемая религия и т. д. На наш взгляд, важным условием создания и использования подобных классификаторов является не нарушение прав и свобод человека.

Далее, фундаментальное право человека на жизнь, свободу и неприкосновенность провозгласила Всеобщая декларация прав человека в статье 3: Каждый человек имеет право на жизнь, на свободу и на личную неприкосновенность. В статье 12 она защитила данное право. Необходимо отметить, что с точки зрения определения право на жизнь и свободу является весьма сложным, так как начинается с элементарных требований жизни: пищи и крова.

Действительно, развитие информационно-коммуникационных технологий позволило увеличить показатели сохранения жизни и здоровья человека. Использование новых технологий значительно повысило уровень медицинских исследований и возможности технических методов обеспечения безопасности в чрезвычайных ситуациях. Экономический эффект от использования информационно-коммуникационных технологий неоспоримо поднял планку качества жизни современного общества. Одновременно с этим те же самые технологии сделали жизнь человека технологически проницаемой, отражая прямую зависимость: чем больше человек пользуется благами и услугами, предоставляемыми современными технологиями, тем его жизнь и личность становятся более уязвимыми как в информационно-технологической, так и в реальной среде. Например, те же самые технологии защиты безопасности, стоящие на страже конфиденциальности коммуникаций человека, модифицированным образом превращаются в технологии наблюдения за его частной жизнью, нарушая все ранее провозглашенные принципы Декларации.

Предоставляемая технологиями безопасная анонимность отнюдь не гарантирует эффективность защиты конфиденциальности личности. Проблема хранения и использования персональных данных частными и государственными учреждениями сегодня вызывает ряд вопросов. Каких обязательств придерживаются частные организации по охране персональной информации? Какие правила оперирования личными данными граждан (особенно в глобальных информационных сетях) действуют для государственных учреждений, существуют ли таковые вообще? Действительно, сама по себе процедура наблюдения является противоречащей идее сохранения прав человека, но при этом необходимо вспомнить о вопросах безопасности, когда записи с камер видеонаблюдения помогали в установлении фактов, событий, личностей, совершивших преступление и т. д. Поднимаемый вопрос, как наглядно показывает практика, требует детального анализа каждого случая. На наш взгляд, возможно, в будущем политика безопасности и внедрения новых технологий потребует согласия с каждого человека о методах и вариантах его участия в системах информационно-коммуникационных технологий.

В то же время не стоит упускать из внимания тот факт, что при всей статистической точности машинный код может содержать ошибки и, более того, может быть намеренно испорченным. Указанное замечание наиболее актуально в вопросах безоговорочного доверия судопроизводства к компьютерным записям и фактам, предоставленным технологическими устройствами с целью сбора «доказательств», что открывает большое число инфоэтических нюансов. Показания человека или свидетельство машины – что заслуживает большего доверия? Это новая дилемма современного общества.

Способы взаимодействия человеческих мыслей, совести и даже религиозных убеждений – еще один вопрос информа-

ционного общества. Статья 18 и статья 19 Декларации прав человека констатируют, что каждый человек имеет право на свободу мысли, совести и религии; право на свободу убеждений и на свободное выражение их, это право включает свободу беспрепятственно искать, получать достоверную информацию и распространять идеи любыми средствами и независимо от государственных границ.

Сегодня информационно-коммуникационные технологии дают возможность каждому человеку общаться на любые интересующие его темы. Однако право свободно выражать свои убеждения в информационном обмене, даже прикрытое анонимностью, достаточно обманчиво. Те же технологии, служащие каналами по обмену информацией, становятся ограничителями информационного содержания[1], в других случаях идентификаторами людей, имеющих альтернативные взгляды, с целью выявления и вмешательства в их жизнь[2]. По поводу вышесказанного В. Зельцер пишет: «Свобода передавать информацию включает право на анонимное выражение мнения; свобода собраний включает право образовывать союзы, не раскрывая имен членов группы; свобода искать и получать информацию включает право слушать, смотреть и читать в частном порядке»[3]. Со своей стороны мы заключаем, что защита анонимности жизненно необходима для демократического государства.

В указанном контексте данная тема, по нашему предположению, тесно переплетается с проблемой защиты конфиденциальности (статья 12) и правом на получение и распро-

[1] Программы фильтры для ограничения информации для граждан через Интернет, устанавливаемые государством [Электронный ресурс]. – URL: http://www/opennetinitiative.org (дата обращения: 12.01.2007).

[2] Судебное заседание по делу диссидентов на основе информации, представленной Yahoo! [Электронный ресурс]. – URL: http://www/rsf.org/article.php3?id_article=16402 (дата обращения: 12.01.2007).

[3] Зельцер В. Анонимность выражения мнения [Электронный ресурс]. – URL: http://wendy.seltzer.org (дата обращения: 22.01.2014).

странение информации (статья 19), где право на свободу убеждений теряет всякий смысл с отсутствием способа выражать это убеждение. Информационные технологии дают право свободно общаться, выбирая форумы, руководствуясь своими убеждениями, но имеют возможность ограничивать общение путем установления фильтров. Таким образом, право на получение и распространение идей в информационном обществе «идет в ногу» со свободой собраний и объединением в союзы, что провозглашено в статье 20.

На наш взгляд, возможность вступить в различные союзы приобретает в информационном мире двоякую зависимость от информационно-коммуникационных технологий. С одной стороны, информационные технологии стимулируют взаимодействие между людьми, существенно облегчая и упрощая его. Однако использование информационных технологий с целью выявления членов свободно организованных ассоциаций и запрета мирных собраний чинит препятствия в реализации идеи свободного обмена информацией. Кроме того, с нашей точки зрения, отдельного решения также требует вопрос, связанный с идентификацией тех, кто воздерживается в желании вступать в какие-либо союзы. Дело в том, что современные условия информационного общества могут нарушать право индивида, ограничивающего свое участие в ассоциациях, осуждая его и принуждая пользоваться преимуществами информационно-коммуникационных технологий. Как уже было отмечено выше, технологии во всех отношениях и смыслах в разы усиливают связь права на личную жизнь или конфиденциальность, описанное в статье 12, с правом, провозглашенным в статье 19 настоящего документа, – на поиск, получение и распространение информации.

В обществе сегодняшнего дня политика и информационные технологии также неразрывно связаны. Политически активные группы широко используют глобальную сеть в по-

исках электората. Лидеры политических партий в качестве основного источника распространения своих убеждений и позиций, с целью координирования действий своих сторонников применяют средства массовой информации и коммуникационные системы. Информационно-коммуникационные технологии, при условии законной реализации данных возможностей, вполне способны воплотить в жизнь все пункты статьи 21, гласящие об избирательном праве каждого человека посредством равнозначных форм, обеспечивающих свободу голосования. В противном случае, необходимо подчеркнуть, демократические выборы теряют смысл. Примером тому могут служить такие действия, как фальсификация результатов электронного голосования или исключение значительного числа групп избирателей из списка политически активных единиц путем лишения доступа к информационно-коммуникационным технологиям и т. д.

Следующая тема касается образования в информационном обществе, которое с внедрением информационных технологий приобретает важнейший статус и значение в социальной жизни человека. Право на образование закреплено в статье 26 декларации. В данном ключе мы выделяем несколько причин, определяющих зависимость современного образования от информационных технологий. В первую очередь рост ценности технического образования, обусловленного масштабным применением технологии во всех областях: «оно (техническое образование) начинает рассматриваться как целесообразный путь развития карьеры…»[1]. Вторая причина заключается в том, что информационные технологии – это неоспоримый источник знаний и один из способов взаимодействия в научно-образовательной среде. Оттого проблема цифрового расслоения общества становится как никогда актуальной в области получения образования, ре-

[1] Этические аспекты новых технологий. Обзор. М. : Права человека. 2007. С. 24.

шать ее – важная государственная задача информационного общества.

Воплощение в жизнь концепции формирования общей информационной среды как источника распространения творческих идей – основная цель внедрения и использования информационных технологий, что отражено положениями статьи 27. Идеи свободного распространения информации и защита авторских прав – поле битвы столкнувшихся интересов в недрах глобальных сетей. Технические средства, позволяющие полноценно взаимодействовать в культурной жизни, или технологии, нарушающие интересы правообладателей? На наш взгляд, найти точки компромисса, определить легитимный путь культурного насыщения каждого индивида – проблема, которую призвана решить информационная этика способом анализа возможностей информационных технологий в отношении соблюдения прав человека.

Так, Декларация прав человека ООН провозгласила в качестве приоритетных целей обеспечение справедливости, свободы и мира. В границах информационной этики идею свободы мы предлагаем конкретизировать в свободе убеждений, совести, доступа к информации, идея справедливости заложена в возможности равного доступа к информации, обеспечение мира кроется в праве на участие в управлении государственных процессов, происходящих в стране. Справедливость, свобода и мир – величины всеобъемлющие и морально приемлемые для каждого. Такой нравственный фундамент для современного общества, с нашей точки зрения, приобретает особенный смысл, поскольку сегодня привычный смысл этих понятий дополнен новыми сторонами равенства и процветания человека.

Таким образом, одной из важнейших задач информационной этики является защита прав и здоровья человека как основного субъекта информационной безопасности, а также реализация его свобод и возможностей (творческих, полити-

ческих, интеллектуальных и т. д.). С целью воплощения вышеуказанных идей, на наш взгляд, современному обществу необходимо обеспечить два обязательных и взаимодополняющих друг друга условия. Первое условие связано с обеспечением максимального разнообразия легитимного контента в информационных сетях, второе условие предполагает гарантию всеобщего доступа к информации и информационным технологиям с целью реализации возможности каждого индивида пользоваться всеми благами от применения информационно-коммуникационных технологий. Рассмотрим основное содержание указанных условий подробнее.

Философия взаимодействия в информационном обществе несет в себе идею максимально разнообразного контента в информационных сетях, отражающего все легитимные интересы и предпочтения пользователей, обеспеченного в результате исключения различных видов контроля и цензуры. Открытость всех возможных источников информации позволяет быть не только пассивным потребителем, но и самому внести посильный вклад в информационное наполнение сети, то есть стать полноправным участником коммуникационного взаимодействия в информационном обществе.

В свою очередь, под видами контроля, на наш взгляд, необходимо выделить цензуру со стороны правительства, предпочтения средств массовой информации, интересы интернет-провайдеров и компаний сотовой связи. По нашему мнению, вопросы использования цензуры и контроля информации исторически варьируются в соответствии с интересами политической, экономической, религиозной и военной мощи государства. Так же не стоит забывать о роли культурных и нравственных традиций в формировании взглядов и предпочтений общества. Проведем различие между понятиями «цензура» и «контроль». Цензура предполагает активное исключение информации по религиозным, политическим, моральным или иным убеждениям, в свою очередь,

направления контроля в выборе информации регулируются в соответствии с целями деятельности, например, учреждения. При этом отметим, что процедуры контроля так или иначе являются предвзятыми в отношении определенных групп контента, что неизменно ведет к потере этического баланса.

В то же время существующие тенденции в либеральных обществах, характеризующиеся меньшим контролем информационного контента, неизбежно ведут к моральным и правовым конфликтам. Применение этических кодексов и международных соглашений – спасение от произвола цензуры и давления контроля, убежден Т. Фрелих[1]. Проблемы, связанные с отсутствием нейтральности в работе классификаторов, тезаурусов, поисковых систем, он предлагает искать не только в предвзятых мнениях или предрассудках, а также в энтропии и различных видах и методах поиска в поисковых системах. Полностью поддерживая автора, мы отмечаем следующие важные факторы в процессе формирования полноценного разнообразия информации и источников, из которых она поступает, – это сохранение «нейтралитета сети» и работа поисковых машин.

Словосочетание «нейтралитет сети» предполагает, что передача информационного трафика в сети осуществляется «вслепую», то есть без учета содержания контента. Сохраняя данный принцип работы, интернет-провайдер обязан передать трафик без идентификации адресата и его содержания. Абсолютно нейтральная к контенту сеть таит в себе опасности, поскольку ее информационное содержание не всегда носит легитимный характер. Здесь может находиться информация различного вида, начиная с тем, оскорбляющих честь и достоинство, до спама и вирусов. По нашему мнению, в

[1] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. – Munich. 1997

борьбе за безопасное содержание информационных сетей с негативными сторонами указанного нейтралитета информационная этика обязана воспитывать в сознании авторов чувство ответственности за содержание предоставляемого контента и стимулировать технологические разработки, целью которых является формирование положительных свойств нейтралитета сети будущих информационно-коммуникационных технологий.

Относительно работы поисковых машин необходимо заметить, что их функционирование самым прямым образом влияет на сохранение разнообразия контента в информационных сетях. Провайдеров интернет-услуг и поисковые машины обычно называют узким местом в потоке трафика и первым регулятором в вопросах доступности контента. Примером тому служит прецедент с компанией «Google». Поисковая машина «Google» фильтровала французские и немецкие сайты на предмет антисемитского или нацистского содержания с целью их удаления[1]. Возможно, с этической точки зрения конкретный пример не подлежит критике, но указанную способность, мы убеждены, необходимо осуществлять в отношении только незаконного содержания.

В вопросах обеспечения разнообразия информации без должного внимания нельзя оставить тему сохранения культурной идентичности в информационных сетях. Культурная идентичность любой страны предполагает уважение к самобытности ее языка в Сети, наличие доменных имен и доступность основного программного обеспечения на всех языках

[1] Рабочий документ для подготовительной группы по правам человека, силе закона и информационному обществу, п. 8, 15 сентября 2004 г. (об осуждении цензуры в действиях поисковых машин во Франции, Германии и Китае) [Электронный ресурс]. – URL: http://cyber.law.harvard.edu/filtering/google/results1html (дата обращения: 02.11.2007).

мира[1]. Наряду с решением социальных, экономических и политических аспектов данного вопроса, специалисты предлагают некоторые технические варианты разрешения указанной проблемы. На наш взгляд, глобальная среда предоставляет возможность для самовыражения каждому человеку, обществу, нации, сохраняя свои исторические, географические культурные особенности. Обеспечить сосуществование этого разнообразия мировых культур в глобальном информационном мире способен межкультурный диалог, поэтому необходимо утверждение и культивирование принципов информационной этики, чтобы цифровые средства стали истинным символом творчества и свободы человека.

Решая проблемы использования информационных технологий исключительно в поддержку прав человека и реализации фундаментальных свобод, в том числе обеспечения безопасности его здоровья, развития творческого потенциала, повышения уровня образования, кроме того, предлагая новые возможности относительно полного участия в культурной жизни информационного общества путем формирования разнообразного контента в информационных сетях, информационная этика обязана обеспечить выполнение второго условия, без практического осуществления которого описанная выше деятельность теряет всякий смысл. Это гарантия всеобщего доступа к информации и информационным технологиям, с целью реализации возможности каждого индивида пользоваться всеми благами информационно-коммуникационных технологий. Возможность каждого индивида в современном обществе использовать последние достижения информационных технологий – задача, требующая

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. – М. : Межрегиональный цент библиотечного содружества. 2009. С. 19.

совместной целенаправленной работы специалистов по информационной этике и правительства.

Этические вопросы, касающиеся доступа к информации, необходимо рассматривать в качестве социальной проблемы создания равных возможностей. Каждый человек в информационном обществе заинтересован и должен быть обеспечен в свободном и равном доступе к информации, а также к свободной коммуникации. В целях обеспечения равного доступа к информации и коммуникации, в первую очередь, необходимо расширить информационную зону общедоступной информации.

Под информационной зоной общедоступной информации предполагается общий объем информации, доступный каждому индивиду. «Информация, являющаяся общественным достоянием – доступная для общественности информация, использование которой не нарушает ни прав, установленных законом, ни обязательств сохранения конфиденциальности»[1]. Данную категорию составляют следующие виды информационных документов: правительственные документы; научные данные; информация, относящаяся к безопасности здоровья; документация, касающаяся информационной безопасности, отражающая современное состояние развития технологий, варианты и методы ведения информационных войн, описывающая реальные и потенциальные опасности, методы защиты от них и другие возможные риски прав индивида; творческие работы в качестве базы для активного взаимодействия в культурной жизни общества.

В свою очередь, с целью расширения возможностей доступа к информационным технологиям, на наш взгляд, необходимо внимательно пересмотреть процессы распространения коммуникационных технологий и развития информаци-

[1] Этические аспекты новых технологий. Обзор. – М. : Права человека. 2007. С. 26.

онных сетей. Так, распространение информационных технологий, обеспечивающих коммуникационные процессы в обществе, напрямую связано с решением проблем информационного неравенства и обеспечения прав человека на общение и участие в информационном взаимодействии. Как показывает практика, понижение стоимости информационных технологий не позволит им стать равнодоступными для всех, это обусловлено, в первую очередь, постоянным возникновением более совершенных разработок на рынке информационных продуктов. Что же касается развития информационных сетей, то здесь для сохранения баланса необходимо максимально исключить влияние отдельных групп, лиц, заинтересованных в воплощении собственных интересов в процессах стандартизации и создании сетевых технологий. Важно стимулировать разработку и использование информационных технологий с выгодой для общества в целом.

Таким примером доступности информационных технологий и внедрения эффективных обучающих средств нового формата может служить программа «Каждому ребенку по лэптопу». Данный проект «One Laptop per Child, OLPC», задуманный Media Lab MIT, впервые был объявлен в 2005 году как попытка начать массовое производство дешевых и надежных лэптопов для распространения их по всему миру с целью повышения качества обучения детей и предоставления возможности исследования, экспериментирования и самовыражения. Распределение компьютеров происходило в Китае, Индии, Бразилии, Аргентине, Египте, Нигерии и Таиланде. Руководители проекта помимо технических задач ставили цели философского характера, «поскольку, принося домой такие компактные устройства, дети приобщали всю семью, при этом чаще всего лэптоп являлся самым необычным и до-

рогим устройством во всей округе»[1]. Кроме того, в вопросе увеличения степени доступности информации необходимо отметить предложение А. Гора, демонстрирующее законодательную инициативу: 0,5-процентный налог («e-rate») в качестве способа субсидировать возможность присутствия в киберпространстве социально незащищенных слоев населения (1988 г.)[2].

Таким образом, мы убеждены, что права и фундаментальные свободы человека, защита которых составляет одну из основных задач информационной этики в рамках информационной безопасности, в целом не должны зависеть от последствий применения информационных технологий. Они представляют собой своеобразный этический минимум, задающий ориентир будущего гуманистического направления развития общества. На основании чего возможно заключить, что новая этика информационного общества способна предвидеть и влиять на результаты использования информационно-коммуникационных технологий.

Так, заранее рассматривая результаты применения информационных технологий через призму ее задач и принципов, у общества появляется вероятность определить возможные последствия их приложений, что увеличивает шанс регулировать гуманистическое развитие информационных технологий в русле использования преимуществ, снижая возможный вред. Важно отметить, что информационные технологии всегда находятся в состоянии постоянного изменения и инновации. Еще десять лет назад едва ли возможно было представить масштабы социальных изменений, которые последуют за внедрением сети Интернет. Даже если общество

[1] One Laptop per Child FAQ [Электронный ресурс]. – URL: http://laptop.org/fag.en_US.html (дата обращения: 08.11.2006).

[2] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный цент библиотечного содружества. 2009. С. 13.

не в состоянии предвидеть все возможные результаты применения информационных технологий, важно попытаться представить вероятные изменения от использования новых технологий. Необходимость в подобной работе верно чувствует Дж. Мур: «философы обязаны обратить особое внимание на развивающиеся технологии и оказать максимальное влияние на разработку этих технологий еще на ранней стадии, до того, как они окажут отрицательное воздействие на человека и его моральные ценности» [1]. Появляющиеся с неизменной скоростью новые решения в области информационных технологий оказывают самое непосредственное влияние на общество, поэтому возникает настоятельная необходимость учитывать последствия их применения. Высокая скорость технологических изменений требует сегодня от человека ответственного использования и предугадывания возможных последствий потенциального влияния информационных технологий уже на стадиях его разработки.

В связи с вышесказанным в целях обеспечения безопасного применения информационных технологий мы видим необходимость в проведении этического анализа новых технологических разработок. В качестве объектов указанного анализа рассмотрены информационные технологии из числа технологий завтрашнего дня[2], являющие собой основу новых способов коммуникаций – новые информационные технологии.

Объектами анализа обеспечения безопасного применения информационных технологий нами выбраны те технологии, которые продолжат реализацию и усовершенствуют базу по формированию интеллектуального пространства, в результате чего еще более приблизят общество к информаци-

[1] Moor J. Why We Need Better Ethics for Emerging Technologies // Ethics and Information Technology. 2005. Vol. 7(3).

[2] Этические аспекты новых технологий. Обзор. М. : Права человека. 2007. С. 12-14.

онному. Перспективы использования следующих технологий в большинстве случаев рассматриваются пока только в будущем, а некоторые из них только предугадываются. Итак, это семантическая сеть и метаданные, управление цифровой идентичностью и биометрия, радиочастотная идентификация (RFID) и датчики, геопространственная сеть и технология LBS (услуги, основанные на технологии определения местоположения), сети с ячеистой структурой, вычисления на основе Grid-технологий и новейшие вычислительные технологии. Опишем в самом общем виде свойства указанных новых технологий.

В качестве положительных аспектов применения описанных технологий необходимо отметить, что перспективы их работы связывают с дальнейшим развитием информационного общества. В первую очередь, использование подобных технологий ведет к увеличению вероятности доступа к информации. В результате расширения возможностей использования информации, бесспорно, повышается эффективность информационного взаимодействия, что ведет к общему экономическому развитию общества и росту уровня жизни, в частности. Грамотное использование описанных технологий позволит существенно оказать помощь в процессе защиты частной жизни и безопасности, оно открывает новые возможности для общения людей со схожими интересами и для свободы собраний. Различные категории населения, по каким-то причинам ущемленные сегодня в возможности использовать средства поиска информации, память для хранения данных и т. д. ввиду отсутствия финансовых средств или географического расположения, с внедрением новых технологий приобретают данное право. Кроме того, процесс использования этих технологий подразумевает расширение круга возможностей государства в сфере оказания услуг населению и создание эффективной системы отчетности, что в идеале должно способствовать соблюдению прав человека.

Новые технологии вооружены арсеналом методов воздействия, стимулирующих выполнение закона, что, несомненно, ведет к повышению общего уровня безопасности. Перспективы их использования в качестве средства спасения людей из неблагоприятных ситуаций в рамках реализации прав человека на жизнь, свободу и безопасность выглядят весьма оптимистично.

В то же время в плане реализации прав и свобод человека результаты применения указанных технологий таят в себе следующие опасности. В первую очередь, необходимо отметить проблемы современных технологий относительно лингвистического смешивания виртуального и реального миров. Сегодня конкретную физическую личность скрывают (или раскрывают?) различные цифровые данные. Управление цифровой идентичностью необходимо понимать как управление цифровой информацией, касающейся конкретного человека. Подобную информацию называют «персональными данными» или «персонально идентифицированной информацией». Прототипом системы управления цифровой идентичностью, являющейся своеобразным словарем метаданных с целью автоматизированного обмена персональными данными, в реальном мире является биометрия, которая, в свою очередь, применяет метаданные к физическому пространству. В свое время Ф. Киттлер связал три категории Лекана – Символическое, Воображаемое и Реальное – с техническими изобретениями [1] . Письменное слово позволяет выразить внутренней голос, чтение – типографически созданная галлюцинация, благодаря которой буквы алфавита перевоплощаются в образы и звуки. Так, мы убеждены, и биометрия в системе с метаданными и механизмом управления цифровой идентичностью расскажет о жизни и предпочтениях каждого

[1] Киттлер Ф. А. Мир символического – мир машины // Философско-литературный журнал ЛОГОС. – М., 2010. № 1(74). С. 5-22.

члена информационного общества, складываясь из цифровых данных физических особенностей человека.

В то же время нами выделены в процессе применения биометрических технологий три новые проблемы, которые уже на сегодняшний день требуют своего решения. Первый вопрос касается центрального администрирования, при условии присвоения государством каждому человеку единственной цифровой идентичности. При решении данной проблемы стоит учесть тот факт, что ни одна организация или международный институт не вооружены механизмами, защищающими от коррупции. Кроме этого, сегодня ни одна организация не в состоянии обеспечить техническую безопасность своих систем.

Второй вопрос описывает ситуацию, в которой человек полностью теряет анонимность, поскольку глобальный идентификатор способен обеспечить возможность создания полного отчета о действиях каждого человека. На наш взгляд, описанная проблема, в свою очередь, порождает явление информационной асимметрии: каждое действие человека записывается без его ведома, что противоречит фундаментальным свободам, таким как право на собрания, поиск информации и обмен ею.

Последний вопрос относится к правосудию: со временем биометрические технологии становятся все более точными, однако к чему могут привести ложные совпадения биометрических данных? Поскольку информационное общество обязано предупредить использование инструментов управления цифровой идентичностью в целях узурпации, дискриминации, а также блокирования коммуникации, здесь серьезно поднимается проблема существования механизмов защиты для неприкосновенности частной жизни и безопасности.

Кроме этого, делегируя машинам функции интеллектуальных агентов, позволяя создавать многочисленные классификаторы, необходимо помнить о такой актуальной теме,

как злоупотребления властью, на фоне которой проявляется проблема взаимодействия между человеческим интеллектом и машинным. Данную проблему, с нашей точки зрения, не стоит относить к вопросам отдаленного будущего. Учитывая масштабы революции в области всеобщей автоматизации, когда человек доверил машине функции: от формирования в сети баз данных различного характера до предоставления веб-услуг, вопрос уже не просто в том, как люди будут использовать данные инструменты, но в том, что будет, если машины оперируют настолько хорошо организованными персональными данными? Зарождение машинного интеллекта, глобального интеллекта Сети – это уже далеко не футуристические идеи из области фантастики, это наше сегодня.

Все вышеуказанное приводит нас к мысли, что процессы идентификации человека вызывают много вопросов. К их числу относится еще один: использование новой RFID-технологии. Сочетание данной новейшей технологии с другими раскрывает ряд широких возможностей для информационного общества: использование RFID-технологий в качестве способа мониторинга и борьбы с распространением вирусных заболеваний; мониторинга уровня активности пожилых людей и людей с хроническими заболеваниями.

Уже не секрет, что такое широкое применение данной технологии может стать поводом возникновения негативных последствий для жизни человека и социума. В первую очередь RFID-технологии создают проблемы для безопасности частной жизни человека, позволяя установить связь между RFID-чипами и отдельными людьми, вовлеченными в процесс их использования. Например, безобидная, на первый взгляд, маркировка потребительской продукции позволяет создавать детальную картину расходов любого частного лица. В свою очередь, использование чипов на рабочих местах дает возможность контроля: информацию, как о месте нахождения, так и о соблюдении правил поведения сотруд-

ников. Кроме этого, нельзя исключать ситуацию, при которой в свете геополитических интересов, стимулируя «гонку контроля», правительства представят требование де-юре или де-факто на вживление в человека имплантата[1]. По нашему мнению, данное требование противоречит всем представлениям о гуманности, так как не исключает возможности психологического давления на людей, лишая их прав на реализацию коллективных действий, защиты частной жизни и свободы собраний. Таким образом, по мере того как технологии осуществляют сбор и хранение данных о деятельности людей на все более высоком уровне, нормы практического применения новых информационных технологий нуждаются в пересмотре.

Следующий вид новейших устройств – датчики, применяемые с целью обнаружения присутствия биологических или химических веществ. С одной стороны, перспективы применения датчиков стоит рассматривать как бесспорный вклад в обеспечение прав человека на жизнь, свободу и безопасность. Сюда относят те случаи, в которых датчики применяют в качестве спасительного средства от вредных химических веществ или природных катаклизмов, в целях предупреждения распространения вирусов на основе местного анализа биологических образцов. Кроме того, датчики могут содействовать решению проблемы неприкосновенности частной жизни путем регистрации нарушений границ частной собственности.

Функции датчиков вполне нейтральны, но в то же время сервис, который предоставляет информацию, полученную с помощью сенсора, вызывает серьезные поводы к беспокойству. Так, например, на основе инфракрасного излучения, фиксируемого датчиками, реализуется возможность выстро-

[1] Wisconsin Bans Forced Human Chipping // Free Market News Network. – 2006. – 1 June.

ить картину действий человека или отслеживать передвижения относительно выделенной зоны. Данная функция легко может служить с целью установления слежения за перемещением отдельно взятого человека или группы лиц, возможно, тем самым ущемляя права определенного сегмента. Другая информационно-этическая проблема касается вопросов, связанных с доступом к информации, являющейся общественным достоянием. В этом случае возникают разногласия по поводу совместного ее использования: кому принадлежат права на данные, предоставляемые сенсорами, или они относятся к сфере общедоступной информации? Каковы последствия трансляции в веб-сетях изображений со спутников, касающейся государственных вопросов конкретной страны и т. д.?

Как известно, новые информационные технологии никогда не поддавались влиянию таких областей, как стандартизация и законодательное регулирование, оттого, по нашему мнению, уполномоченные лица и специалисты в области информационных технологий должны реально оценивать возможные последствия результатов использования сенсорных технологий, создавая благоприятный климат для решения возникающих вопросов с позиции информационной этики.

Если сенсорные датчики дают нам количественную информацию о реальном мире и обрабатывают ее в данные, которые считываются машинами, то геопространственная сеть и технологии LBS преобразуют этот процесс, применяя цифровые данные к определенным объектам реального мира, путем сочетания данных, взятых из разных источников.

Не оставляет сомнений тот факт, что использование геопространственной сети и технологии LBS оказывает содействие здоровью и безопасности человека, предоставляя новые возможности для коммуникации. Однако это убеждение верно лишь при условии разумного решения этических вопросов их применения, в противном случае те же самые

права и свободы человека будут подвергнуты опасности. По нашему мнению, необходимо обратить особое внимание на противоречивые возможности использования указанных технологий, которые заставляют задуматься над следующим вопросов. Кто имеет право обладать информацией о местоположении другого человека? Кроме того, необходимо помнить, что с точки зрения защиты неприкосновенности частной жизни контроль над местоположением частного лица является явной угрозой наблюдения и примером дискриминации, а в некоторых случаях и причиной угнетения. В процессе широкого применения технологий LBS для определения местонахождения индивидов, объединения их функций с датчиками и биометрией человек постепенно лишается свободы выбора в вопросе: кому и когда открывать информацию о своем местоположении?

Кроме того, мы особо выделяем, что нельзя оставлять без внимания проблемы автоматизации данного процесса, заключающиеся в программировании машин на более аккуратную работу с персональными данными. Наделение программ управлять подобной информацией должно заставить человека задуматься об их программировании на определенный уровень интеллектуализации в работе с персональными данными. Что же касается вопросов безопасности и хранения полученных данных, то использование привычной установки компьютерных кодов лишь поднимает новый вопрос о праве собственности на данную информацию и контроле над ней. Таким образом, как показывает анализ применения LBS-технологий, здесь весьма актуальна тема установления юридических и технологических механизмов безопасности, вызванных обеспечить приемлемое использование информации о местонахождении конкретного лица.

Активное внедрение ранее описанных технологий, дало идею создания коммуникативной сети, связывающей все технологии воедино. В то же время функционирование мас-

штабной Grid-системы не лишено недостатков, обмен вычислительной мощностью и данными скрывает в себе много проблем, связанных с безопасностью. В особенности это касается, на наш взгляд, процесса протекания аутентификации, точнее, его централизованного характера, который теоретически может привести к угрозе дискриминации отдельных групп пользователей сети доверенными лицами, в чьих руках сосредоточено управление. Другая группа вопросов в плане безопасности личности и общества затрагивает архитектуру Grid-сетей, подразумевающую различие контента за счет «глубокой пакетной проверки» правительством и интернет-провайдерами, что, в свою очередь, позволяет указанным структурам контролировать содержание информационного трафика. «Жесткая централизация и сосредоточение контроля в одном месте позволяет использовать информацию ради собственных нужд, ограничивать для других количество и качество информации, злоупотреблять «секретностью», то есть создавать дискриминацию в отношении нового вида ресурсов»[1]. Данная ситуация, без сомнений, является примером прямой угрозы праву свободы слова.

Подводя итог о работе новой технологии, мы подчеркиваем, что в основе развития такой инновации, как Grid-сеть, лежит тот же самый принцип, который был основополагающим в период зарождения Интернета, – нейтралитет сети по отношению к разным типам информации, основная идея которого заключена в том, чтобы сеть всегда оставалась нейтральной для содействия развития коммуникации при условии «интеллекта, находящегося по обе стороны», то есть там, где осуществляется соединение пользователей.

Проведенный анализ новых технологий подводит нас к следующему заключению: миссия глобального внедрения

[1] Management of government information systems, elements of strategies and policies. N. Y. : United Nations. 1999. P. 75.

информационных технологий, рассмотренных в анализе обеспечения безопасного применения информационных технологий для общества и человека, несет в себе много спорных моментов. Несмотря на все перспективы внедрения новейших технологий, к возможным отрицательным последствиям относят повышение поляризации в обществе и влияние на свободу убеждений, что, соответственно, неизбежно ведет к нарушению общественного диалога. Необдуманное применение новых технологий способствует дискриминации, а также увеличивает угрозу несанкционированного раскрытия или потери защищенной информации. В данной ситуации не исключается возможность возникновения системы государственного контроля, злоупотребления властью и создание условий для масштабного наблюдения, что нарушает право на невмешательство в частную жизнь, свободу собраний и слова и т. д. Кроме того, возникают серьезные причины для беспокойства по поводу сохранения государственного суверенитета и безопасности, а также относительно нарушения общего геополитического баланса.

Еще одна возможная проблема, на которую, с нашей точки зрения, стоит обратить особое внимание, заключается в потенциальной угрозе зависимости в информационном обществе людей от машин, уже сегодня действующих от их имени в качестве агентов. Как отмечают специалисты[1], по мере развития информационного общества компьютеры чаще будут брать на себя обязанность формирования словаря метаданных, которые на лингвистическом уровне приравнивают каждого человека реального мира к объектам информационного потока. С целью решения проблемы приоритетности данных необходимо адекватно программировать машины, в результате чего информация о людях будет размещена на более высокий уровень, чем данные об объектах. Компь-

[1] Этические аспекты новых технологий. Обзор. М. : Права человека. 2007. С. 84.

ютерная лингвистика должна научиться описывать человека не в контекстуальных терминах, а в терминах, связанных с существенными, неотъемлемыми и постоянными атрибутами индивида. В таких случаях, когда компьютеры запрограммированы на особо бережное отношение к данным о человеке, они автоматически должны оцифровать биометрическую информацию на совершенно другом уровне, чем при обработке данных о неодушевленном предмете.

Действительно, технологии формирующегося общества обещают развитие новых форм контента и возможностей. В свою очередь, перед человеком стоит задача уже сегодня принять верные решения в отношении использования этих технологий. Адекватное программирование информационных технологий должно создаваться уже сегодня человеком, который руководствуется информационно-этическими принципами и моральными нормами. От решений сегодняшнего дня зависит формирование глобального виртуального мозга, который направит свою интеллектуальную мощь на реализацию защиты человека и его прав, и в результате – на устойчивое состояние информационной безопасности общества. Новые технологии могут быть использованы для решения многих задач, оттого важно принять подходы в их использовании, максимально минимизирующие отрицательные социальные и этические последствия. Правильный выбор информационного общества заключается в социальном программировании мощных машин будущего на уважение ценностей человека.

Таким образом, в рамках информационной безопасности определена важная задача информационной этики, содействующая развитию процесса гуманизации социума – основным приоритетом применения информационных технологий на службе обществу и государству являются защита прав и фундаментальных свобод человека. В целях достижения поставленной задачи определены два необходимых взаимодо-

полняющих друг друга условия: обеспечение максимального разнообразия легитимного контента в информационных сетях и обеспечение всеобщего доступа к информации и информационным технологиям.

Высокая скорость новых решений в области информационных технологий оказывает самое непосредственное влияние на человека и общество в целом, от того возникает настоятельная необходимость учитывать последствия их применения благодаря анализу и программированию возможностей информационных технологий на уважение человеческих ценностей. В результате чего информационное общество обязано обеспечить в качестве одного их приоритетных направлений государственной политики организацию и поддержку научных исследований в области разработки и внедрения информационных технологий, а также всестороннего анализа и прогноза результатов ее использования. Используемые обществом информационные технологии должны получать социальное содержание и воплощать цели, исключающие антигуманистическое применение.

Сегодня, в условиях коренных изменений всех социально-культурных процессов в обществе, нравственные, гуманистические аспекты развития информационных технологий требуют своего отражения в нормативном регулировании феномена информационной безопасности.

3.2. ПРАВОВЫЕ НОРМЫ И САМОКОНТРОЛЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Действие информационных технологий должно быть безопасным для человека и общества. В предыдущем параграфе мы отметили, что не стоит упускать из внимания ни один из видов информационных опасностей: недостаточная защищенность, злоупотребление властью, неправильное или

непредусмотренное использование технологий, а также излишняя централизация информационных операций администрацией и т. д. Теоретик права Л. Лессиг справедливо констатирует: темпы изменений в области информационных технологий происходят настолько быстро, что оставляют совещательный процесс законодательства далеко позади, в результате чего остаются вне закона[1]. Действительно, на сегодня одними из главных препятствий эффективного функционирования в информационной среде остаются вопросы, связанные с принятием законов и развитием человеческого фактора.

Важно отметить, что информатизация вызвала юридические проблемы в таких областях, как тайна, безопасность данных, межграничные информационные потоки, контрактное право, собственность, защита авторских прав и патентов, компьютерные преступления и правонарушения. Информационные технологии создают возможность записи, хранения и манипуляции информацией разных видов – не только фактами и цифрами, но и визуальной информацией, графиками, речью, поскольку информационные технологии позволяют практически мгновенно передавать неограниченные массивы информации на любое расстояние с любого терминала сети. В связи с этим государственная политика должна направляться на поиск нового юридического оформления этого феномена.

Воздействие информационных технологий убедило правительственные организации в необходимости рассчитывать долгосрочные последствия при определении правовой регламентации функционирования информационных систем. Попытки наложить новую культуру на существующие правовые порядки в тех областях, где широко применяются информационные технологии, не могут оставаться без измене-

[1] Lessig L. Code and Other Values of Cyberspace. N. Y. : Basic Books. 1999.

ний, поскольку прежние правовые доктрины теряют свое действие. Такие оформившиеся области права, как конституционное, контрактное, патентное и авторское, претерпели серьезные перемены. Компьютерные преступления значительно изменили структуру уголовного процесса и уголовного кодекса, поскольку существовавшие юридические нормы не предусматривали наказания за «высокотехнологичные» преступления.

Рассматривая сложившуюся ситуацию в области правового регулирования в сфере информационной безопасности, на наш взгляд, необходимо выделить два основных аспекта, требующих своего ключевого решения. Первая группа проблем относится к вопросам исполнения правового законодательства в сфере информационных технологий. Специалисты отмечают трудности в реализации государственных законов в информационном пространстве, а также несовершенство самого законодательства в вопросах идентификации компьютерных преступлений и определения наказания[1].

Вторая категория проблем вытекает из вопросов урегулирования национальной законодательной базы с международной практикой. Интернационализация Интернета подрывает принципы контроля и соблюдения национального законодательства, рождает противоречия в определение юрисдикции при решении технических, экономических, культурных и т. д. вопросов функционирования в информационной среде. Интернет ставит государства в совершенно иное положение друг к другу, требуя качественно иного, более высокого уровня международного взаимодействия и госу-

[1] Шамраев А. В. Правовое регулирование информационных технологий. Анализ проблем и основные документы. М. : Статус, 2003; Zittrain J. Internet Points of Control. In The Emergent Global Information Policy Regime, edited by Sandra Braman. – Houndmills: Palgrave, 2004; Рассолов И. М. Право и Интернет. М. : Норма. 2003; Бабкин С. А. Интеллектуальная собственность в Интернет. М. : Щит-М. 2006 и др.

дарств, и международных организаций. Существование Интернета порождает целый комплекс задач и вопросов[1], решение которых лежит в плоскости международного права.

При этом важно сказать, что описываемые аспекты находятся в тесной взаимосвязи, например, несовершенство и несогласованность принятого национального законодательства с международными нормами отражается в правовой международной практике, в свою очередь, международное право накладывает свои ограничения на решения национального правового регулирования.

Рассмотрим особенности правового регулирования в области информационной безопасности, обусловленные уникальной спецификой информационных технологий. Из истории информационной безопасности известно, что в 60-х годах прошлого столетия технология создания глобальной компьютерной сети изначально не предполагала обеспечение принципов безопасности, сеть строилась в качестве электронного средства передачи файлов между исследовательскими группами[2]. Первые попытки формирования структур защиты информации и компьютерных систем в некоторых важных областях были предприняты позже: Закон об инфор-

[1] Касенова М. Б. Интернет и международное публичное право: ретроспектива доктринальных подходов [Электронный ресурс]. – URL: http://lexandbusiness.ru/view-article.php?id=577 (дата обращения: 25.05.2014); Наумов В. Б. Право и Интернет: очерки теории и практики. М. : Книжный дом «Университет». 2002; Mayer F. C. The Internet and Public International Law-Worlds Apart? // European Journal of International Law (EJIL). 2001. Vol. 12. № 3; Reidenberg J. Technology and Internet Jurisdiction // University of Pennsylvania Law Review. 2005. Vol. 153; Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur, 1997; Benkler Y. The wealth of networks : how social production transforms markets and freedom (1st ed.). New Haven, Conn: Yale University Press, 2006.

[2] Зегжда П. Д., Зегжда Д. П., Семьянов П. В. Теория и практика обеспечения информационной безопасности. М. : Яхтсмен. 1996.

мационных записях и свободах (Франция, 1978 г.), Акт о данных (Швеция, 1973 г.), Закон об общественных информационных системах (Югославия, 1981 г.), Акт о защите федеральной компьютерной системы (США, 1984 г.). Далее, всеобщая информатизация и компьютеризация, а также масштабное развитие компьютерной сети Интернет открывают новую главу в области информационной безопасности. Информационная революция, благодаря возникновению новых видов атак и нарушений, привлекла вновь обострившееся внимание к старой дискуссии о жизненной безопасности государственной системы и общества в целом.

В этой связи важно отметить, что романтика, характерная для расцвета эпохи информационных технологий и сети Интернет 1980–1990 годов прошлого столетия, сформировала представление об электронном пространстве, созданном на базе указанных технологий, как о царстве свободы и неограниченных возможностей. Общее мнение того периода выражало надежды в способности преодолеть границы территориального права, ведущие к потере прежнего смысла государства как такового. В литературе в вопросах управления электронной средой отразились предсказания о потере прежних полномочий государством в эпоху цифровых технологий и господство полной автономии в пространстве Интернет. Футуристы, в том числе Дж. Барлоу, Д. Негропонте, Э. Тоффлер, оптимистично предрекали конец государственного управления, которое Д. Барлоу описывает как «тиранию», обращаясь к правительствам индустриального мира: «Вы не имеете морального права ни управлять нами, ни обладать любыми методами правоприменения. Киберпространство лежит вне ваших границ»[1]. Д. Негропонте считал, что государство будет сокращаться в условиях глобализации, за-

[1] Barlow J. A Declaration of the Independence of Cyberspace // Declaring Independence. 1996. № 4.06. W.

явив, что никто не имеет «рецепта для управления подобным миром, поскольку киберзаконы (cyberlaw) более глобальны»[1]. Социологи были полны надежд, полагая, что интернет-технология воплотит в жизнь прямую демократию для народа, подарит возможность непосредственно участвовать в процессе принятия решений[2].

Мы приходим к выводу, что энтузиасты раннего периода сети Интернет строили новую парадигму организации человеческого общества на основе информационных технологий в виде отдельного и самостоятельного виртуального мира[3], деятельность которого не требует привычного вмешательства со стороны органов власти. Новая философия объясняла ситуацию относительно определения юрисдикции интернет-пространства особой природой глобальной сети, требующей полной свободы для своих пользователей. Утверждалось, что идея введения юридического контроля над информационными коммуникациями здесь будет заранее обречена на провал, поскольку традиционное применение территориальных особенностей права разрушено[4]. Таким образом, ситуация, в которой философия информационного взаимодействия отвергает факт какого-либо регулирования, подкрепленная отсутствием изначально заложенных принципов безопасности в технической архитектуре глобальной сети, послужила поч-

[1] Цит. по: Flichy P. The Internet Imaginaire. London, UK, Cambridge, MA: The MIT Press. 2007. P. 117.

[2] Hague B., Loader B. Digital Democracy. Discourse and Decision-Making in the Information Age. L., N. Y. : Routledge. 1999.

[3] Barlow J. A Declaration of the Independence of Cyberspace // Declaring Independence. 1996. № 4.06. W.; Dibbell J. A Rape in Cyberspace: How an Evil Clown, A Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society [Электронный ресурс]. – URL: http://www.juliandibbell/com (дата обращения: 21.05.2014); Reidenberg J. Rules of the Road on Global Electronic Highways: Merging the Trade and Technical Paradigms // J. Law & technology. 1993. P. 287.

[4] Post D., Johnson D. Law and Borders – the Rise of Law in Cyber space // Stanford Law Review. 1996. № 4. P. 1237.

вой для усугубления противоречий и конфликтов в современном информационном пространстве.

Позже, с увеличением числа преступных проявлений вседозволенности и анонимности в исследованиях пионеров киберпространства наблюдается значительная трансформация взглядов, говорящая о смене свободных настроений в сторону необходимости принятия регулирования. В данном дискуссионном поле заводится речь о специфическом характере среды Интернет, предполагающем собственное особое регулирование [1]. Так, появляется понятие «интернет-контроль»[2], сфера деятельности которого распадается на три измерения: доступ к сети, функциональность электронной сети и деятельность в информационном пространстве. Большинство из проблем, попадающих в сферу данного контроля, имеют, на наш взгляд, нравственный и социальный характер, например, наблюдение, в том числе и за частной жизнью, онлайн-мошенничество и кражи, информация, оскорбляющая достоинство человека и общественные нравы, экстремистская и расистская пропаганда, практические пособия для создания оружия, взрывных зарядов и т. д. Подчеркнем тот факт, что принятие решения об особом контроле глобального пространства является значительным сдвигом в общественном сознании к пониманию всей важности и необходимости государственного регулирования процессов, протекающих на основе информационно-коммуникационных технологий.

Кроме того, существует еще один важный аспект: современный мировой порядок образован при помощи автоматизированных кибернетических систем, управляемых компью-

[1] Post D., Johnson D. The Great Debate – Law in the Virtual World // First Monday. 2006. Vol. 11(2). P. 1230; Benkler Y. The Wealth of Networks, How Social Production Transforms Markets and Freedom. New Haven, Conn: Yale University Press. 2006.

[2] Eriksson J., Giacomello G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State // International Studies Review. 2009. Vol. 11(1). P. 206.

терами. Участниками информационного взаимодействия сегодня также являются интеллектуальные машины. Благодаря чему, подчеркнем эту мысль, полномочия могут быть перенаправлены, осуществлены и, более того, извращены с помощью дистанционного управления через автоматизированные системы или интеллектуальных агентов. В ответе на вопрос: «кто» или «что» управляет и контролирует в технологически опосредованной кибернетической практике? – сделать какие-либо различия становится все труднее. Напомним предвидение Д. Харауэй: «новые машины двадцатого века сделали неоднозначной разницу между естественным и искусственным, ума и тела… Наши машины обладают все увеличивающимся арсеналом возможностей, при этом мы сами пугающе инертны»[1]. В данной ситуации необходимо обратить особое внимание на возможности кибернетических систем, логистики, микрочипов, гибридов при анализе работы глобальной электронной сети, которая представляет собой своеобразную технологическую карту. Включения указанных «негосударственных субъектов» в информационное взаимодействие становятся неизбежными в жизни цифрового человека и социума, не исключен тот факт, что подобные кибернетические организмы и искусственные интеллекты незаметно, но эффективно переопределят ручное управление, тем самым делая государство и гражданское общество устаревшими. В результате этого вопрос о государственно ориентированных понятиях управления (власти, влияния, контроля) электронно-компьютерной средой более чем актуален.

В поиске ответа на вопрос, что означает глобальная диффузия Интернет: конец способности государства контролировать общество или, наоборот, государство укрепляет свои позиции в обществе, с нашей точки зрения, необходимо

[1] Haraway D. J. Simians, Cyborgs and Women: The Reinvention of Nature. N.Y. : Routledge. 1991. P. 225.

отвергнуть романтические абстракции о глобализации и трансформации власти в пространстве, образованном информационными технологиями. Более того, национальные законы, традиции и обычаи наряду с технологическими решениями важны в киберпространстве так же, как и в реальном мире.

Государственно ориентированная точка зрения гласит, что умение влиять и следить за соблюдением законов является ключом к решению многих проблем в глобальном пространстве. Осмысление процесса управления электронной средой предполагает триаду независимость - дисциплина – правительство[1], которая в своей основе имеет цель – обеспечение интересов общества и реализацию механизмов безопасности. Актуальность рассматриваемого вопроса возрастает с признанием прямой взаимосвязи регулирования киберпространства с состоянием информационной безопасности, значит, и национальной безопасности страны.

В сфере информационной безопасности важной областью законодательства становится борьба с информационными, или компьютерными, преступлениями, осуществляемыми на базе глобальной сети. Компьютерная преступность наносит большой ущерб, но при этом установить факт совершения преступления весьма сложно. Ввиду отсутствия свидетельств назвать даже приблизительное число совершаемых преступлений невозможно. Эксперты считают подобного рода преступность серьезной проблемой и оценивают ущерб в несколько миллиардов долларов в год[2]. Информационный мир живет по собственным законам и правилам, в котором классические схемы криминалистической экспертизы

[1] Eriksson J., Giacomello G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State // International Studies Review. 2009. Vol. 11(1). P. 215.

[2] Фролов Д. Б., Старостина Е. В. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Законодательство и экономика. 2005. № 5.

не действуют. Федеральное бюро расследований полагает, что в США лишь 1 % компьютерных преступлений обнаруживается и лишь о 12 % из них сообщается. В России статистика показывает, что шесть из восьми лиц, обвиняемых в хакерском нападении, избегают своего наказания[1].

В данном ключе нам необходимо указать, что среди специалистов нет единства относительно определения состава компьютерных преступлений[2]. Утверждения традиционных законов о собственности, которую можно украсть, которая должна быть ощутимой (вещественной) и при краже изменить владельца, в случае с такими категориями, как программное обеспечение и базы данных, теряют всякий смысл. Например, в Швеции более широко используется термин «компьютерные злоупотребления», которые, в общем, определяются как инцидент, связанный с компьютерной технологией, в котором жертва терпит или может потерпеть убытки, нарушитель извлекает или может извлечь выгоду. Компьютерное преступление может совпадать со следующими признанными категориями преступлений: финансовые преступления, кража собственности и вандализм. Кроме того, встает вопрос об оценке украденной собственности, который позволяет дифференцировать крупные и мелкие преступления при вынесении наказания.

Существующие законы относительно хищений, вторжения в частную жизнь, нарушения конфиденциальности, торговых секретов, авторского права и подделок документов, использующиеся для наказания компьютерных преступлений, вызывают в ходе реализации ряд трудноразрешимых вопросов. Например, в случае обвинения в хищении торго-

[1] Официальный сайт МВД России [Электронный ресурс]. – URL: http://mvd.ru (дата обращения: 09.01.2014).

[2] Карамнов А. Ю., Дворецкий М. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах // Вестник ВИ МВД России. 2011. № 2.

вых секретов может возникнуть вопрос о «незащищенном вскрытии». На наш взгляд, подобная ситуация возникает при отсутствии должного внимания к мерам защиты со стороны собственника информации, которую похитили, в таких случаях закон не имеет силы.

Другой проблемой является несанкционированный доступ к файлам сверхсекретной важности, даже с целью только демонстрации способностей индивида преодолевать меры безопасности. В чем состав преступления, если информация не стиралась, не копировалась и не использовалась? Возможно, наиболее эффективные способы уголовного наказания будут обнаружены при детальном рассмотрении криминального компьютерного поведения в квалификации наказаний и идентификации преступлений. Здесь необходимо заметить, что наказание за различные типы информационных правонарушений, например, за несанкционированный доступ, не затрагивает вопросы, касающиеся «осязаемости» краденого и признаков «обладания», которые являются определяющими при рассмотрении обычных краж.

В этой связи можно выделить некоторые специфические различия в определении преступлений в информационной среде из международного законодательства. Так, юридическая практика в США с 1984 года квалифицирует компьютерные преступления на два вида компьютерных правонарушений: против интеллектуальной собственности и против несанкционированного использования информационной технологии[1]. Федеральный закон Австралии называет уголовным преступлением несанкционированный доступ к компьютерам, особенно обслуживающим системы связи и транспортные коммуникации. Практика Китайской Народной Республики подразделяет компьютерные преступления на два

[1] Management of government information systems, elements of strategies and policies. N. Y. : United Nations, 1999. P. 174.

вида: преднамеренное заражение системы компьютерным вирусом, распространение нелицензированных программ. Гонконг разработал ряд нормативных документов, предупреждающих совершение компьютерных преступлений. Согласно их трактовке несанкционированное проникновение через информационно-коммуникационные системы в компьютер является уголовным преступлением, сюда также относят взлом компьютерной системы с целью получения выгоды или нанесения ущерба[1]. Модельный Уголовный кодекс стран СНГ преступления в информационной сфере трактует как преступления против информационной безопасности[2].

Уголовный кодекс Российской Федерации нарушения в области информационной безопасности определяет как «преступления в сфере компьютерной информации»[3]. По определению В. Л. Кудрявцева, преступления в сфере компьютерной информации – «это общественно опасные деяния, предусмотренные Главой 28 Раздела IX УК РФ, посягающие на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств, хранения, обработки и передачи»[4]. Рассуждая над смыслом данного определения, укажем на тот факт, что формулировка «преступления в сфере компьютерной информации» обладает двойственным значением: часто ее отождествляют с термином «компьютерные преступления». При этом классификация преступлений в данной области включает преступления

[1] Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М. : Книжный мир. 2009.

[2] Модельный Уголовный кодекс стран СНГ [Электронный ресурс]. – URL: http://online.zakon.kz (дата обращения: 16.01.2014).

[3] Уголовный кодекс Российской Федерации. М. : Проспект, КноРус. 2010. С. 129.

[4] Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика//Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки применения его положений с учетом задач дальнейшего укрепления экономического правопорядка. Н. Новгород. 2012. С. 69.

в сфере компьютерной информации в число вторых, отчего рассматриваемое понятие приобретает широкий и узкий смыслы[1]. Мы приходим к следующему выводу: отсутствие точной формулировки, оптимально отражающей все особенности феномена, запутывает и, возможно, накладывает некоторые затруднения в определение объекта преступления.

Из всего вышесказанного можно заключить следующее: имея общие цели и задачи в борьбе с компьютерными преступлениями, уголовные законодательства государств существенно отличаются[2]. Каждая страна дает свое определение преступлениям в информационной среде, а также определяет размер наказания, в то же время общая характеристика проблем примерно одинакова. На фоне отдельных нюансов правового регулирования каждого государства одним из важнейших вопросов для всех стран международного содружества остается проблема реализации законодательной базы страны в глобальной среде.

Серьезным аспектом указанного вопроса является проблема урегулирования законопроектной системы с международной практикой. Дело в том, что юристы многих стран рассматривают вопросы обработки межграничного потока данных в соответствии со своими политическими, культурными традициями. В тех странах, где присутствует федера-

[1] Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика//Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки применения его положений с учетом задач дальнейшего укрепления экономического правопорядка. Н. Новгород, 2012. С. 69.

[2] Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. № 11; Карамнов А. Ю., Дворецкий М. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах // Вестник ВИ МВД России. 2011. № 2; Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки применения его положений с учетом задач дальнейшего укрепления экономического правопорядка. Н. Новгород. 2012.

тивное устройство, законодательство усложняется. Межграничные потоки данных, то есть электронная информация, курсирующая через национальные границы с целью хранения, обработки и дальнейшего использования, – важная проблема для многих стран, поскольку законы, рассчитанные на соблюдение их на определенной территории, в этом случае не действуют.

Необходимо отметить, что в поисках решения проблем в области международного регулирования работы глобальной сети и процесса использования информационных технологий выделился один из наиболее «удобных» подходов – это координирование технических аспектов, в том числе и установление универсальных стандартов. Формирование взглядов о том, что сеть Интернет представляет собой, прежде всего, техническую конструкцию, привело к идее управления в новом формате. Так, теория Л. Лессига предполагает в качестве правил контроля технические протоколы и программное обеспечение, являющие собой архитектуру сети, которая в роли «особых правовых норм»[1] обязана регулировать свободу поведения пользователей. Характер и особенности будущей сети, а значит и свободы, которые она может гарантировать человеку, зависят от построения архитектуры Интернета. В этой связи Й. Эриксон выразительно замечает, что универсальные технические протоколы сети несут не меньшее значение, чем генетический код организма человека[2].

Действительно, технические компоненты глобальной сети в различных аспектах отвечают государственной юрисдикции, позволяя контролировать условия безопасности в вопросах контента, доступа к информации и т. д. Кроме того, основные технические характеристики информационно-

[1] Lessig L. Code and Other Laws of Cyberspace. N. Y. : Basic Books. 1999. P. 61.
[2] Eriksson J. Cyberplagues, IT, and Security: Threat Politics in the Information Age // Journal of Contingencies and Crisis Management. 2001. Vol. 9(4).

компьютерной коммуникации, оформленные в виде коммуникационных протоколов, снижают стоимость и повышают эффективность. Так, ряд оценочных стандартов и спецификаций[1] внесли свой невосполнимый вклад в формирование научно-методологической базы в области информационной безопасности: они раскрывают понятийный базис, регламентируют важные технические аспекты, дают практические рекомендации по поддержанию безопасного режима и т. д.

Между тем техническая сторона вопроса далеко не единственная проблема обеспечения безопасности, к тому же, как показала практика применения информационных технологий, в стандартизированные компьютерные системы легче проникнуть злоумышленнику.

Анализируя проблемы глобализации с точки зрения юридической ответственности, Т. Фрелих выделяет следующие вопросы: Кто должен контролировать информацию (контент и/или программное обеспечение), приходящую из разных стран на территории интернета? Как национальные законы, будучи географически ограничены, смогут ответить

[1] Критерии оценки доверенных компьютерных систем – стандарт Министерства обороны США (англ. Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, DoD 5200.28-STD, December 26, 1985) [Электронный ресурс]. – URL: http://mind-control (дата обращения: 05.02.2013); Гармонизированные критерии европейских стран (Information Technology Security Evaluation Criteria, ITSEC) [Электронный ресурс]. – URL: https://www.bsi.bund.de-/SharedDocs/publicationFile (дата обращения: 05.02.2013); Руководящие документы Гостехкомиссии России [Электронный ресурс]. – URL: http://www.ivtechno.ru/files/rd_filter.pdf (дата обращения: 05.02.2013); Критерии безопасности информационных технологий» Федеральный стандарт США (Federal Criteria for Information Technology Security) [Электронный ресурс]. – URL: http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf (дата обращения: 05.02.2013); Общие критерии оценки безопасности информационных технологий» международный стандарт (Common Criteria for Information Technology Security Evaluation Security) [Электронный ресурс]. – URL: http://www.ipa.go.jp/security/jisec/cc/documents-/CCPART1V3.1R4.pdf (дата обращения: 05.02.2013).

на вызовы в киберпространстве?[1] Специалисты обеспокоены проблемами юрисдикции: Каким принципам нормативно-правового поля должен соответствовать контент – «страны-производителя» или «страны-получателя»? Каковы пределы компетенции относительно информации, доступной в нескольких странах?[2] Так, вопросы изучения различных аспектов правового регулирования в области информационных технологий, в том числе анализ согласованного действия международного права и глобального пространства, становятся одними из центральных тем в современной научной литературе.

В этом ключе выделим исследование П. Майера относительно ограничений, налагаемых международным правом, в котором он приходит к заключению о выделении основных направлений в области стабилизации: разработка общих принципов деятельности, международные соглашения в сфере коммуникаций, общее международное договорное право, а также общие межгосударственные инициативы в сфере координирования деятельности сети Интернет[3]. Мы согласны с мнением автора в том, что выработка общих принципов регулирования деятельности в информационной среде станет основой анализа многих актуальных вопросов: киберпреступность, риски нападения на критические точки государств и т. д. Применение положений договорного права окажется полезным в поддержке конвенционных норм относительно прав человека и основных свобод в информационном веке. Принятые договора международных союзов могут составить

[1] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. – Munich: G. K. Saur, 1997.

[2] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный цент библиотечного сотрудничества. 2009. С. 35.

[3] Mayer P. Das Internet im offentlichen Recht. Unter Berucksichtigung europarechtlicher und volkerrechtlicher Vorgaben. Berlin: Duncker & Humblot, 1999.

основу информационного взаимодействия, например, международных инструментов, совершенствующих работу в области передачи информации и т. д. Кроме того, необходимо утвердить права и обязанности различных международных организаций относительно координации вопросов об администрировании в среде Интернет, разработки технических стандартов, функционирования телекоммуникационных рынков.

Поддерживает тезис о создании международного договора Э. Лонгворт, по его мнению, он должен выявлять основные моменты правового режима и систему урегулирования споров в международных судах. Вывод работы заключается в разработке многогранной структуры децентрализованного управления сетью Интернет, требующей максимальной концентрации стараний многих стран для сохранения международного диалога в области перечисленных вопросов. В свою очередь, Дж. Голдсмит и Т. Ву поощряют данную идею: децентрализованное управление эффективнее стимулирует свободу, разнообразие и самоопределение[1]. Кроме того, Э. Лонгворд видит особые перспективы в разработке концепции информационного пространства в качестве международного на примере международных вод Антарктиды[2]. Так же Э. М. Бальсано предлагает положения об околоземном пространстве применить к решению вопросов в поле сети Интернет[3]. Таким образом, постановка вопроса о подписании международных договоров в поиске общих принципов регулирования электронно-компьютерного пространства с целью формирования межгосударственного сотрудничества в правовой сфере логична и обоснована, это многоаспектная

[1] Goldsmith J., Wu T. Who Controls the Internet?: Illusions of a Borderless World. N.Y.: Oxford University Press. 2006.
[2] Les dimensions internationales du droit du cyberspace. Publio sous la direction de Teresa Fuentes-Camacho // Editions UNESCO. 2000. P. 11.
[3] Ibid. – P. 127.

и сложная проблема, требующая глубокого и обстоятельного изучения.

Со своей стороны, продвигая идею подобного подхода, выделим причины, объясняющие необходимость применения межгосударственных документов:

- предотвращение принятия несовместимых местных законов;
- содействие выработке единых стандартов на законодательные акты в области информационных технологий.

Многоаспектное изучение перспектив правового государственного регулирования сети Интернет позволяет заключить, что практика применения подобного подхода требует дальнейших исследований. На наш взгляд, только всестороннее изучение вопроса, включающее такие аспекты, как морально-этические, культурные и т. д., позволит найти наиболее эффективные приемы и методы регулирования социального взаимодействия в информационной среде. Уважать заданные положения в условиях постоянного ужесточения внутренних и международных требований к безопасности становится актуальнейшей задачей современного общества. Описанная ниже ситуация ярко демонстрирует результат применения в юридической практике сугубо технических решений в исследуемых проблемах.

Как оказалось, современный мир глобальных сетей дает дополнительную возможность для злоумышленников совершать компьютерные атаки не только в пределах собственной страны. В тех случаях, когда какое-либо государство не предусматривает наказания в сфере компьютерных преступлений, оно имеет право не оказывать содействие в расследовании преступлений. Так, с целью решения вопросов о международном сотрудничестве в борьбе с правонарушениями в информационной среде Совет Европы подписал Конвенцию о преступности в сфере компьютерной информации (ETS № 185 23 ноября 2001 г.). Основной задачей данного документа

явилось создание правовых условий в киберпространстве. В результате все преступления в интернет-пространстве были разделены на четыре группы, для предотвращения которых налагались определенные требования странам, подписавшим конвенцию. В то же время некоторые общественные организации (США, Великобритания, Испания) сформулировали обращение, выражающее протест против действия требований конвенции[1], поскольку увидели в ряде ее положений противоречия статье о защите прав человека Европейской конвенции. В частности, такие действия интернет-провайдеров, как фиксация и перехват при помощи технических средств информации для правоохранительных органов, воплощают в нормы практики контроль над частными коммуникациями. Стоит предположить, что вопросы в сфере правового урегулирования отношений в информационно-компьютерной среде еще не проявили всю свою палитру красок и послужат поводом для многих дебатов.

С точки зрения гармонизации национальных законов и международных правовых норм функционирования в информационной среде специалисты[2] определяют наиболее важные направления применения общих принципов действующих правовых актов в сфере использования информационных технологий. К числу наиболее актуальных для рассмотрения проблем необходимо отнести следующие: обеспечение безопасности и тайны данных; признание прав на данные.

Как показывает мировая история защиты данных, безопасности информации всегда уделяли значительно больше внимания, чем их доступности. Например, в Великобритании был принят Официальный секретный акт (1911 г.), во Фран-

[1] Electronic Frontier Foundation [Электронный ресурс]. – URL: https://www.eff.org (дата обращения: 10.01.2012).
[2] Management of government information systems, elements of strategies and policies. N.Y.: United Nations, 1999. P. 156.

ции – Закон об архивах (1760 г.) и Закон о секретной статистике (1957 г.) в отличие от первого в юридической практике Закона об информации, записях и свободах, принятого в 1978 году. Опыт также свидетельствует, что односторонняя и не контролируемая со стороны общества концентрация информации в государственных базах данных может усилить бюрократическую и технократическую власть администрации. Поэтому многие страны приняли законы, обеспечивающие свободу информации. Например, в Швеции гарантируется право доступа к общественным записям и документам, которые получают, издают или обрабатывают центральные или местные органы власти.

Вопрос, касающийся тайны данных, раскрывает проблему создания общих юридических принципов относительно сохранения тайны данных, или, иначе, конфиденциальности информации. Тайну данных можно определить, как способность индивида контролировать использование относящейся к нему информации[1]. Использование информационных технологий при обработке данных о личности, усложнение компьютерных систем и сетей отчетливо обозначили проблему сохранения тайны данных. Одно фундаментальное положение гласит: обладание информацией о личности оборачивается властью над ней, что превращает вопрос о неприкосновенности данных в одно из основных прав человека. Например, культурные традиции Китая, Таиланда и Японии, опирающиеся на религиозные каноны, с наступлением информационного века терпят трансформацию взглядов на частную информацию о личности, что неотъемлемо отражается в нормативно-правовой базе охраны данных.

С появлением сети Интернет, в 90-х годах прошлого столетия правовая база Китая ввела четыре принципа, форми-

[1] Management of government information systems, elements of strategies and policies. N. Y. : United Nations. 1999. P. 170.

рующих защиту данных по примеру западной позиции: принцип уважения, принцип информированного согласия, принцип равновесия (между защитой частной жизни и общественной безопасностью), принцип социальной ректификации (очищения)[1]. В Таиланде, стране, не имеющей отдельного закона, защищающего персональные данные, правительство намерено ввести цифровые карты, удостоверяющие личность человека. С. Хонгладаром, в свете угроз конфиденциальности частной жизни своих сограждан, дает следующее обоснование нововведению: «Тот факт, что буддизм отвергает идею индивидуального "я", не означает, что он отвергает частную жизнь»[2]. «Аналогичные натяжки» анализируют в культурной жизни японского общества, убеждающие то, что сегодня каждый живет в системе трех миров: «сакаи», «секен» и «икаи», порождая сложную дискретную идентификацию личности[3]. Первый из миров ассоциируется с влиянием современных западных ценностей, второй символизирует традиционное мировоззрение, третий олицетворяет зло и все вытекающие из него бедствия объективного и субъективного характера. Так, на наш взгляд, с пониманием необходимости защиты персональных данных в современном цифровом мире восточное мировоззрение, разительно отличающееся от западной субъективности, принимает систему глобального информационного взаимодействия.

Сегодня информация о личности попадает в чрезвычайно разветвленные сети, сложность и возможности которых выходят за рамки понимания. При этом передача данных базируется исключительно на доверии к государственным орга-

[1] Lü Y. Privacy and data privacy in contemporary China // In Ethics and Information Technology. 2005. P. 7-15.
[2] Hongladarom S. Analysis and Justification of Privacy from a Buddhist Perspective. – Information Technology Ethics: Cultural Perspectives: Idea Group. 2007. P.122.
[3] Nakada M., Tamura T. Japanese conceptions of privacy: An intercultural perspective // In Ethics and Information Technology. 2005. P. 27-36.

нам и уверенности в том, что с подобной информацией обращаются должным образом все участники информационных отношений, что она находится под охраной закона и ее нельзя использовать в целях, наносящих какой-либо вред индивиду. Вопрос обеспечения тайны данных становится особенно важным в условиях функционирования автоматизированных информационных систем. Скорость, многосторонность, гибкость, мощность современных технологий в сочетании с низкой стоимостью значительно облегчают создание обширных систем записи, банков данных, что позволяет информации о личности становиться максимально доступной и уязвимой. Возможности информационных технологий позволяют непредсказуемым образом сочетать данные, кроме того, к ним могут получить доступ лица и организации, не имеющие на это права и использующие их в своих иных целях, нежели это предусматривалось. Тайна и безопасность данных неразрывны. Поэтому, с нашей точки зрения, важной задачей государственной политики современного общества является осуществление баланса между правом человека на защиту от злоупотреблений данными, относящимися к нему, и опасностью несанкционированного доступа к конфиденциальной информации.

В связи с тем, что вопрос о конфиденциальности информации личного характера становится одной из центральных проблем информационного общества, правительства разных государств разрабатывают соответствующие нормативные документы о защите тайны данных финансовых и банковских институтов. Например, закон о модернизации финансового обслуживания Грэма – Линча – Блайли раскрывает принципы сохранения конфиденциальности данных о клиентах. Кроме того, в 1996 году США был принят Закон о подотчетности документации о страховании здоровья (Health Insurance Portability and Accountability Act), который ввел стандарты безопасности, оберегающие конфиденциальность

подобной информации. Защита информации о здоровье – основная цель этих положений: конфиденциальность, целостность и доступность данных.

Законодательство Германии отличается развернутым Законом о защите данных, содержащим 44 раздела, расставляющих приоритет в ходе расследования информационных преступлений между национальными интересами и соблюдением тайны частной жизни. Необходимо отметить, что общие требования закона о защите информации Германии (2009 г.) аналогичны положениям действующего закона «О персональных данных» (№ 152–ФЗ) в России в отличие от схем работы подобных законодательных актов в США и Великобритании. Дело в том, что механизм формирования данных здесь имеет схожие черты: в России и Германии не существует «быстро монетизируемых» персональных данных, таких как номер соцстрахования (SSN) в США и номер медицинского страхования (NHS) в Великобритании, которые пользуются определенным спросом на черном рынке. Данный факт иначе называется «кражей личности» (identity theft). Не вызывает сомнений то, что он открывает для злоумышленников новое поле деятельности в сфере мошенничества.

В целях повышения эффективности мер информационной безопасности мы видим необходимость в выделении общих принципов, действие которых должно отражаться в практике законодательной базы каждого государства международного сообщества, заинтересованного в развитии правового регулирования сбора, обработки и распространения данных:

- Обеспечение интересов общества и государства, заключающееся в определении законом доступа к данным, имеющим конфиденциальный и личный характер; предотвращение случайного вмешательства и модификации инфор-

мации в базах данных; разумное регулирование цен на доступ к информации и информационным услугам.

- Обеспечение интересов субъектов данных, предполагающее информирование о видах персональных данных, вводимых в систему, о том, кто, когда, с какой целью и в какой промежуток времени их использует; проведение персональных исследований только в той степени и с той целью, с какими они разрешены в рамках сохранения прав и основных свобод человека; использование строго определенного объема данных, необходимого для известных и разрешенных целей; обеспечение полноты, точности и соответствия времени данных, содержащихся в информационных системах; предоставление права и возможности субъектам данных ознакомиться с информацией, относящейся непосредственно к ним; предоставление субъектам данных права и возможности на исправление данных о себе.

На наш взгляд, можно выделить пять основных прав, касающихся тайны данных: право контроля, право на извещения, право на правильное использование, проверку и право на изменение данных. Таким образом, мы убеждены в том, что вопрос безопасности данных и их сохранности предполагает, что все попытки расширить информационный обмен должны основываться на развитии правовых положений, включающих соблюдение кратких правил: сохранение высокого уровня секретности в отношении определенных категорий информации; использование данных только в законных целях, определяемых законодательством страны происхождения или использования; защита важной информации разумными юридическими и техническими мерами безопасности.

Следующий вопрос относительно обеспечения необходимого контроля безопасности затрагивает тему признания прав данных. Признание прав данных в первую очередь предполагает действие авторских прав, лицензий и ограни-

чений по отношению к определенным видам информации с целью достижения максимально эффективного функционирования информации.

Традиционно законодательство об интеллектуальной собственности (патентное, авторское право) применялось для защиты скорее носителя информации, чем самого содержания. Ситуация изменилась, когда данные были освобождены от своего физического выражения. Сегодня любой желающий может прочесть книгу, не приобретая ее. «В продаже информации заложен внутренний парадокс. Покупателю, узнавшему, что он покупает, уже не нужно покупать эту информацию, так как он ее уже имеет. Во-вторых, хотя создание и приобретение информации может быть весьма дорогим, получив, ее можно весьма дешево воспроизводить»[1].

Актуальнейший вопрос современного общества о защите интеллектуальной собственности мы считаем одним из самых сложных с моральной и правовой точки зрения в области производства информации. Анализ традиционных воззрений в отношении собственности[2], характерных для отдельных регионов мира, приводит к выводу о сложившихся особенностях законодательства защиты авторских прав в сфере информационных продуктов. Так, Европейская традиция, сосредоточенная на обеспечении моральных прав автора, озабочена целостностью связи «личность автора – авторская работа – репутация». Англо-американская традиция в данном вопросе выделяет понятие «имущество», как следствие – имущественные права, то есть авторское право. Согласно данной традиции, «оригинальные авторские произведения, выраженные в любых материальных средствах»

[1] Management of government information systems, elements of strategies and policies. N. Y. : United Nations. 1999. P. 170.

[2] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur. 1997.

(UCC, 1952 г.) должны быть защищены. Азиатские традиции, в свою очередь, рассматривают процесс копирования программных продуктов как процесс эмуляции мастера. В данной группе законотворчество находится под влиянием нравственных традиций, имеющих собственный этический взгляд на различные аспекты информационного взаимодействия.

На сегодняшний день теория информационной безопасности выделяет наиболее слабые места защиты прав на интеллектуальную собственность, характеризующиеся следующими положениями: существующее законодательство применимо к различным проявлениям информационной технологии в большинстве случаев лишь по аналогии; вследствие развития новых технологий воспроизведения информации права на интеллектуальную собственность практически невозможно защитить[1]. Яркими примерами вышесказанного служат все типы компьютерных записей, разработанные программистами, которые, при желании, должны подлежать защите авторским правом. Однако здесь мы отметим, что данное право не предполагает защиту идей и не дает право контроля над распространением проданного материала, поэтому, возможно, желательный уровень юридический защиты следует искать не только в авторском праве, но и в совокупности с такими способами защиты, как лицензирование и лизинг.

В странах, где приняты юридические нормы с целью защиты тайны информации, важную роль в обеспечении интересов производителей интеллектуальной собственности приобретает закон об утрате конфиденциальности. Он применяется к широкому ряду информационных материалов, таких общепринятых, как формулы, чертежи, производственные секреты, списки потребителей, финансовая информация, но

[1] Бабкин С. А. Интеллектуальная собственность в Интернет. М. : Щит-М. 2006.

также дополнительно включает следующую категорию – секреты личного свойства. Действия закона распространяются на письма, бумаги и переговоры (прямые, пересказанные или записанные). При этом нам необходимо указать, что большинство стран, регулирующих обращение с конфиденциальной информацией, сочли непрактичным разработку детальных правил обращения с различными видами информации, будь то государственная, коммерческая, финансовая или частная информация. Что признано целесообразным, так это наличие достаточно гибкой правовой основы, распространяющейся на любую информацию. В данном ключе намечена тенденция сочетать Закон о нарушении конфиденциальности с правилами безопасности. Однако на этом пути важно помнить, что стремление защитить информацию обязано не только ограничиваться требованиями военной или национальной безопасности, но и распространяться на защиту частной жизни, защиту от убытков, мошенничества, злоупотреблений и т. п.

Таким образом, на наш взгляд, сегодня с целью проведения эффективной юридической практики в сфере информационной безопасности для достижения минимальной защиты от информационных преступлений каждому государству необходимо иметь ряд соответствующих законов:

- требования по безопасности и сохранности данных, основанные на международных технических стандартах;
- законы, гарантирующие пользователям применение юридических инструментов в необходимых случаях, защищающих интересы граждан;
- законы и правила, регулирующие межграничные потоки данных и гарантирующие сохранение национальных интересов в информационной сфере для каждой страны.

В то же время стоит отметить, что само по себе законодательство, посвященное отдельным видам преступлений, не способно решить проблему компьютерной преступности как

побочной проблемы эпохи информационных технологий, и как части общего криминального ландшафта. В этой связи одной из главных забот правительства в деятельности по предотвращению информационных преступлений должны стать постоянный контроль и анализ возможных рисков, то есть определение потенциально уязвимых мест в информационных системах от случайных или преднамеренных угроз. Стратегия, направленная на принятие соответствующих мер, снижающих возможные риски, должна включать выявление факторов уязвимости в информационной сфере, подготовку персонала, разумный контроль, предотвращение злоупотреблений или неправильного использования информации. В свою очередь, в целях предотвращения или выявления информационных преступлений построение системы информационной безопасности должно основываться на принципах организации и алгоритмах функционирования современных операционных сред и оболочек, использующих в своей основе максимально возможный уровень системных программных средств и технологий.

Так, информационное общество, на наш взгляд, в целях реализации эффективно действующей системы информационной безопасности обязано разработать и обеспечить успешное функционирование двух следующих групп мер. Первая группа мер направлена на формирование в обществе негативного образа нарушителя информационной безопасности, помимо этого она включает четко сформулированные санкции и наказания за отдельные виды нарушений. Вторая группа содержит координирующие меры, направленные на повышение уровня информированности и образованности общества в сфере информационной безопасности. В итоге совокупное функционирование перечисленных мер должно стать определяющим в процессе обеспечения информационной безопасности, поскольку выделенные меры заблаговре-

менно предупреждают появление различного характера нарушений в информационной среде.

Важно помнить, что борьба с преступностью в области информационной безопасности – это вопрос ограничения риска, нежели победы в войне. Мировому сообществу для управления указанным риском необходима правовая система и эффективный инструментарий, предполагающий достаточный объем знаний у каждого из пользователей. Обществу необходимо выработать творческие подходы для повышения уровня понимания проблем и методов борьбы с преступлениями в информационной среде. В данном контексте, мы подчеркиваем, речь идет о решении вопросов уязвимости путем применения не только технических средств, но этических требований, подкрепленных соответствующими юридическими нормами.

М. Фуко сказал: Государство не имеет сущности. Государство не является универсальным. Государство само по себе не является автономным источником власти. Государство есть не что иное, как эффект, контур, движущееся сечение вечного процесса формирования Государственного[1]. Постигая глубокий смысл сказанного выше утверждения, мы констатируем: признание первостепенной роли моральной ответственности в формирующейся ситуации, обязывает информационное общество создавать механизмы саморегулирования в процессе использования информационных технологий и социального взаимодействия в глобальной среде. В стремлении усовершенствовать действие общего законодательства в сфере информационной безопасности социальные, коммерческие организации и образовательные учреждения должны активизировать свою деятельность по принятию уставов этики и профессионального поведения. Указанные действия еще раз подтверждают мнение К. Маркса о том, что

[1] Foucault M. The Foucault Reader. N. Y. : Pantheon Books. 1984.

моральную силу невозможно создать только параграфами закона. По убеждению Л. Лессига, именно кодекс, в качестве норм и правил, создаст необходимый формат регулирования электронной среды[1]. Так, в первую очередь этические кодексы направлены на более детализированное представление имеющейся регламентации в информационной сфере и реализации возможности способствовать большей саморегуляции пользователя в данной среде.

Обобщение опыта в соотношении с принятыми в обществе моральными нормами, определение общих принципов и правил поведения в процессе взаимоотношения людей в определенной сфере деятельности положили начало формирования кодексов этического поведения. Понятие «кодекс» предполагает систематизированный единый законодательный акт, регулирующий какую-либо однородную область общественных отношений, так же совокупность правил и убеждений[2]. История возникновения кодексов имеет давние традиции, уходящие в религиозные каноны.

В профессиональных сообществах первые кодексы этического поведения были выражены в профессиональных этических нормах, отражающих специфические особенности какой-либо профессиональной деятельности на базе существующих общих нравственных ценностей. Ранние примеры формирования подобных правил, задающих определенные нормы поведения специалистов, встречаются в Древнем Египте, тесно переплетающие моральные требования с правовыми нормами в рамках трудовой деятельности[3]. Также необходимо выделить наследие древнегреческой культуры – «Клятва Гиппократа». Классический свод этических принципов, применяемый по сей день в медицинской практике, при-

[1] Lessig L. Code and Other Values of Cyberspace. N. Y. : Basic Books. 1999. P. 89.
[2] Большой энциклопедический словарь. М. : Сов. Энциклопедия. 1991. Т. 1. С. 597.
[3] Белякова Г. И. Профессиональная этика. М. : Знание. 1975. С. 12.

равнивает медицину к мудрости, а владеющего ей – к богу. Убеждения в презрении к корысти, пороку и суеверию, возвышение скромности, совести и веры в высокие идеалы внушали гордость к профессии и уважение окружающих к особому статусу врача. В Средние века разделение труда в Западной Европе положило начало развитию профессиональных этических требований и уставов. Данный процесс был вызван потребностью в дополнительном регулировании профессионала в специфических обстоятельствах, обусловленных родом его деятельности. Так, профессиональная этика регулирует человеческие взаимоотношения внутри профессиональной деятельности, отражая сущность профессии в качестве совокупности ценностей и идеалов, представляющих профессиональную мораль и задающих нормы профессионального поведения, направленные на повышение эффективности производства результатов.

Важным аспектом, на наш взгляд, является тот факт, что основы профессиональной этики представлены духовными, нравственными идеалами, заложенными в психологии коллектива. Как утверждает Р. Г. Апресян, система этических норм и правил профессионального поведения в сообществах направлена на формирование «должного» с целью достижения «блага»[1]. Особенности этических кодексов складываются в результате специфики какого-либо рода деятельности, например, в сфере медицины, социального обслуживания, воинской службы, СМИ, спорта. Этические кодексы выполняют две важные функции: они регулируют поведение людей и несут представление о социальной ответственности специалистов, выраженной в качестве и достоинстве профессиональной деятельности.

В свою очередь, предназначение теории социальной ответственности состоит в задаче совместить такие принципы,

[1] Apresyan R. G. Ascenso a la moral. M. : Editorial Progresso. 1991.

как свобода личности, свобода медиа и долг перед обществом. Диапазон применения подобной либеральной концепции оказался весьма широк, поскольку охватывал практически все общественные институты вещания. Основные принципы теории социальной ответственности Д. Маккуэйл описывает в качестве высоких профессиональных стандартов объективности и правдивости, продиктованных заботой о благе народа и сохранением баланса между разнообразием существующих точек зрения в обществе, с целью избежать всякого рода насилия или возможности оскорбить группы меньшинств[1]. На наш взгляд, теория социальной ответственности, прежде всего, показывает, что нравственное регулирование процессов в информационной сфере становится необходимым атрибутом демократического общества.

Позже, с развитием информационных технологий, в профессиональных сообществах зарождается потребность в формировании моральных принципов создания и применения этих технологий. Возросшая роль информационных технологий не только преобразует общество в целом, вызывая рост числа занятых в информационной сфере, появление новых профессий, связанных с предоставлением услуг, но и оказывает влияние на менталитет, систему предпочтений, определяющих механизм принятия решений и образ действия человека. Меняются ценности, ассоциирующиеся с организацией труда, взаимодействия человека и машины. Доказательством этого служит практика профессиональных организаций в области информационных технологий, признавших необходимость принятия стандартов профессиональной ответственности для специалистов[2].

[1] McQuail D. Mass Communication and Public Interest: Towards Social Theory for Media Structure and Performance // Polity Press. 1994.

[2] Gotterbarn D., Miller K., Rogerson S. Software Engineering Code of Ethics // Information Society. 1997. № 40(11); Anderson R., Johnson D., Gotterbarn D., Perrolle J. Using the New ACM Code of Ethics in Decision Making // Communications of the

Далее, в период 90-х годов 20-го столетия этическое регулирование выходит за границы сугубо профессиональной среды людей, непосредственно участвующих в разработке информационных технологий. Данное событие ознаменовано включением ряда нормативов в базовый курс образовательных учреждений[1]. Так, постепенно, с распространением информационно-коммуникационных технологий, становление информационного общества потребовало выхода понятий «ответственность» и «нравственное регулирование» за рамки только профессиональной этики. Теория компьютерной этики, стремительно развиваясь, переросла в обширную и актуальную научную область – информационную этику. Сегодня ее предлагают рассматривать как составляющую социальной этики. Механизм институционализации социальной этики содержит важный принцип: в социальной жизни практика индивида осуществляется относительно моральных ценностей, отражающих общественные интересы[2], что, на наш взгляд, отвечает постулатам информационной этики.

Т. Фрелих, размышляя над способами эффективного регулирования информационного взаимодействия, в том, что существует два пути его осуществления: правовое регулирование на национальном, международном уровне и самоконтроль[3]. Под самоконтролем автор концепции предполагает принятие этических кодексов и простое выполнение правил

ACM. 1993; Gotterbarn D., Rogerson S. Responsible Risk Analysis for Software Development: Creating the Software Development Impact Statement // Communications of the Association for Information Systems. 2005. № 15(40).

[1] Turner A. J. Summary of the ACM/IEEE-CS Joint Curriculum Task Force Report: Computing Curricula, 1991 // Communications of the ACM. 1991. № 34(6).

[2] Васильевене Н. Влияние классического философского наследия на развитие прикладной этики (на примере этики организаций) // Философия и этика: сборник научных трудов. К 70-летию академика А. А. Гусейнова. М. : Альфа-М. 2009. С. 671.

[3] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur. 1997.

сетевого этикета. В связи с тем, что глобальное информационное пространство породило большое количество вопросов, с разрешением которых не успевает государственное законотворчество, возникает острая потребность в принятии обществом морального саморегулирования, подтверждающего слова мудреца: там, где в силу не вступил закон, на смену ему приходит мораль.

Поскольку информационная этика имеет дело с социальными проблемами, связанными с киберпространством и обществом всемирной компьютерной сети (networked society), в ней решается, прежде всего, вопрос о том, что представляет собой киберпространство – «среду» или «место»[1]. Если киберпространство больше всего напоминает физическое место, то в рамках этики требуется формирование кодекса с целью определения, как прав, так и обязанностей, ответственности пользователей Интернет[2]. Например, кодекс чести собственников, владельцев и пользователей открытых информационных систем (в том числе интернет-сообщества). Формирования подобного объединения единомышленников в пределах определенной информационной территории уже существуют: Кодекс поведения в Интернет (Канада), Хартия Интернет (Франция). К существующим общим предписаниям в этой области относят основные принципы: свобода мнения; защита частной сферы; защита человеческого достоинства. Эти принципы закреплены и в праве ЕС.

Для России, не имеющей признанного на определенном уровне документа, регламентирующего поведение в информационной среде, основой выработки такого кодекса может стать «Национальный кодекс деятельности в области информатики и телекоммуникаций», принятый торгово-

[1] Tavany H. T. Cyberethics and the future of computing // Computers a. Society. N. Y. 1996. Vol. 26. № 2.

[2] The electronic grapevine: Rumor, reputation a. reporting in the new on-line environment. New Jersey: Mahwah. 1998. P. 199.

промышленной палатой Российской Федерации[1] или разработка Информационной доктрины России[2]. Также в качестве примера указанного выше подхода можно рассматривать фрагменты документа, одобренного Национальной комиссией США по библиотекам и информационной науке (от 29 июня 1990 г.) «Принцип обеспечения доступности информации». Этот документ иначе называют Биллем о праве информации в эру информации. На наш взгляд, Информационная доктрина России должна стать своеобразной «информационной конституцией», из которой вытекали бы не только базовые принципы технократического развития и правового обеспечения информационной деятельности, информационной безопасности, но и морально-нравственные принципы, критерии существования цивилизованной информационной среды общества и государства. В качестве центрального предмета в ней должны быть проработаны общечеловеческие нравственные цели и задачи информатизации, информационной безопасности, ориентированные на обеспечение цивилизованного уровня информационного бытия каждого жителя страны, а далее всего глобального информационного сообщества.

Существующий разрыв между реальностью среды Интернет и провозглашенными этическими принципами в договорах, конвенциях и законодательных актах требует необходимость применения на практике четких правил и точных директив. Ученые мирового сообщества убеждены: «Необходим динамичный, гибкий международный инструмент в виде этического кодекса Интернета с открытыми принципа-

[1] Лопатин В. Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации (проект). М. : Космосинформ. 1998.

[2] Белов Г. В. Парадигма Информационного общества и становление информационного права // Теория и практика общественно-научной информации. М., 2003. Вып. 18.

ми для содействия будущему прогрессу и новым форматам»[1]. Новаторская среда Интернета требует универсального механизма регулирования собственных специфических процессов. По нашему мнению, принятый документ должен ясно и точно отражать предписания, сохраняя особое отношение к таким характерным для среды и весьма спорным с правовой точки зрения нюансам, как, например, индивидуальная собственность или «горизонтальные эффекты». «Горизонтальные эффекты» связаны с позитивными обязанностями государства (понятия, восходящие к конституционному и международному праву), гарантирующими уважение и обеспечение прав человека как в реальной, так и в информационной среде, придание моральным нормам и ценностям интернационального значения.

В связи с признанием факта, что последствия применения информационных технологий вызывают глубокие изменения в обществе, международная организация ЮНЕСКО разработала Этический кодекс информационного общества[2], который призван регулировать отношения в информационном мире. Принципы Этического кодекса утверждают, что информационное общество должно основываться на общепринятых ценностях, все заинтересованные стороны продвигают общественное благо и способствуют предотвращению злонамеренного использования информационных технологий. Однако, при всей важности и необходимости создания подобного документа, в связи с охватом большого числа аспектов жизни информационного общества и чересчур общего

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный центр библиотечного сотрудничества. 2009. С. 37.

[2] Этический кодекс для информационного общества (проект) [Электронный ресурс]. – URL: http://www.osu.ru/docs/kodeks_ethics_info.doc (дата обращения: 30.08.2008).

характера рекомендаций, проект Этического кодекса сочли «неспособным решить существующие проблемы»[1].

По мнению экспертов, из-за расплывчатых деклараций этические кодексы получают большое количество негативных отзывов: «Несмотря на разнообразие кодексов этики трудно выделить документ, который мог бы служить эталоном при разработке стандартов этического поведения в области информационной безопасности. Многие кодексы не отражают специфики профессии, они содержат слишком общие каноны, которые охватывают обязательства любого профессионала: честность, компетентность, ответственность, повышение квалификации и т. п.»[2].

Более того, С. Шварц говорит о принципиальной слабости этических кодексов, которые не способны отразить суть этических аспектов, так как этика изначально не может быть кодифицирована [3]. Он выражает сомнение относительно предполагаемого эффекта от применения этических кодексов: хороший человек и квалифицированный профессионал в одном лице попросту не нуждается в них, а «плохие парни» не будут их придерживаться в любом случае. Дж. Лэдд также придерживается мнения о том, что этические принципы слишком сложны, чтобы быть формализованными [4]. Он рассуждает о плюсах и минусах процесса применения этических кодексов: коды поведения, возможно, будут вдох-

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М.: Межрегиональный центр библиотечного сотрудничества. 2009. С. 14.

[2] Малюк А. А., Полянская О. Ю. Кодекс этики в сфере информационных технологий как основа обеспечения информационной безопасности [Электронный ресурс]. – URL: http://library.mephi.ru/data/scientific-sessions/2007/z14/2-1-23.doc (дата обращения 05.02.2014).

[3] Schwarz S. Research, integrity and privacy. Notes on a conceptual complex // Social Science Information. 1979. № 18 (1).

[4] Ladd J. The quest for a code of professional ethics: an intellectual and moral confusion. In Johnson D.G., Snapper J. W., Eds. Ethical Issues in the Use of Computers. Belmont: Wadsworth, 1985.

новлять на «этическое поведение», консультировать и предупреждать. При этом они способны порождать побочные эффекты: вызывать чувство самоуспокоенности, скрывая «безответственное» поведение, и, что более важно, по его мнению, могут выступать в качестве защитного механизма, отвлекающего от реальных этических проблем.

С нашей точки зрения, важно отметить следующий момент: в данном случае ключевой вопрос заключается не в создании кода, но в содействии обсуждению этических вопросов, связанных с определенной деятельностью. Если этические принципы рассматриваются в качестве аргумента, то они открыты для дальнейшего обсуждения, как само слово «oughts»[1], выражают не «конец», а «начало». Кодексы не являются абсолютным основанием, введенным в качестве закона, они свободны от догмы и выражают человеческую свободу, открытость миру и друг к другу. В этом ключе весьма уместно мнение С. Шварца о том, что этический дискурс – прежде всего, пруденциальный дискурс. «Благоразумие есть добродетель, то есть источник действия, который характеризует положение того, кто осознает его и его ограничения. Это ограничивает антикритерий “все позволено”, информирует о двойственности ситуации»[2]. Таким образом, пруденциальный этический дискурс выполняет функцию сохранения этической чувствительности, результат которой моральная ответственность.

В связи с указанными замечаниями придание этическим кодексам следующих важных характерных особенностей, возможно, по нашему мнению, решит проблему повышения эффективности принятых кодексов.

[1] Schwarz S. Research, integrity and privacy. Notes on a conceptual complex // Social Science Information. 1979. № 18 (1).

[2] Capurro R. Technics, Ethics, and the Question of Phenomenology // Tymieniecka A.-T., Hrsg.: Morality within the Life- und Social World. Analecta Husserliana XXII. – Dordrecht: Reidel. 1987.

1. Первая характеристика, присущая этическим кодексам, обязана отражать их прагматичность, основу которой составляют четкие принципы и установки относительно функций определенной группы действующих субъектов или определенного сектора.

2. Следующая особенность связана с активным привлечением различных профессионалов или заинтересованных лиц к процессу дискуссии о моральных обязательствах, составляющих этический свод правил, в зависимости от их предмета или сферы. Например, в решении проблем ощущения ложного чувства свободы от рамок (социальных, семейных, профессиональных), корректирующих поведение пользователя в информационной среде, призвать к дискуссии этологов, психологов, психиатров. При разработке этических кодексов, регулирующих электронную торговлю, пригласить на обсуждение его положений потребителей, прямо заинтересованных в принятии подобного документа. Результатом этого будет созданный диалог открытых групп, пропагандирующих принципы легитимности и гласности. Подобное многостороннее обсуждение на различных уровнях фундаментальных нравственных принципов послужит приданию этическим кодексам истинной глобальности.

3. Важной характеристикой этических кодексов должно также являться содержание, отличающееся не просто соответствием существующим правовым нормам, но, более того, укрепляющее их и воплощающее в действительность: «Важно, чтобы он был неким дополнением (к законодательным нормам), продиктованным заботой об уважении фундаментальных принципов, которые вдохновляют его: уважении до-

стоинства и автономности личности, солидарности и социальной справедливости»[1].

В свою очередь, проведенное исследование онтологических оснований этических кодексов в ходе исторического развития выявило смену базисных предпосылок к «коммуникативности» от предыдущих «рациональности» и «традиционности», в результате чего пришло к заключению об актуализации процесса формулирования устойчивых ориентиров в социально-неустойчивой среде, характеризующей современную меняющуюся действительность[2]. Мы можем заключить, что в настоящих условиях трансформирующейся реальности этический кодекс является результатом коммуникации, а не ее предпосылкой. Одновременно на кодекс возложена рефлексивная функция, позволяющая проецировать цели системы на поведение каждого индивида, формировать единое поле мировосприятия, что является одним из показателей ее высокого коммуникативного онтологического статуса. В итоге коммуникация приобретает завершенный характер, что свидетельствует о сохранении фундирующей функции этического кодекса. Соответственно, информационная этика, выполняя свою нравственно-регулятивную функцию, наряду с традиционно принятой моралью и правом является механизмом, реализующим формирование нравственной среды в информационном пространстве современного общества.

В данной связи обостряется потребность в изучении и пропаганде принципов информационной этики, содействии ее институализации и усовершенствовании разработанных

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный центр библиотечного содружества. 2009. С. 15.

[2] Черепанова М. В. Актуализация этических кодексов в контексте современной культуры // Известия ТПУ. 2013. Т. 322. № 6. С. 95.

кодексов этического поведения в информационной сфере[1]. Так, в качестве одного из инструментов, исследующих современные кодексы этики, предложен системный подход, который «демонстрирует их функциональные особенности и условия реализации глубинного коммуникативного потенциала, позволяя избежать косности и симулятивности в процессе разработки и практического внедрения»[2]. Более того, с точки зрения системного подхода этический кодекс выступает предпосылкой формирования целостной личности. Это связано с тем, что самоидентификация в новых условиях сопряжена, с одной стороны, с опорой на уже существующие культурные образцы, с другой – на трансформацию наличных смысловых структур. Процессы пересекаются в коммуникативном пространстве, в результате чего формируется новый социальный субъект, «при этом и понимание социальности, и интерпретация субъективности также подвергаются пересмотру»[3], а этический кодекс становится источником новых ценностей, возникающих в ходе поиска индивидом собственной идентичности.

Таким образом, с широкомасштабным применением информационных технологий, с учетом огромного влияния результатов их использования на жизнь современного общества, значение этических кодексов только возрастает, что, прежде всего, связано с повышением числа принятых норм и уставов регулирования человеческого взаимодействия в информационном мире. Основная роль этических кодексов концентрируется на выполнении нравственно-регулятивной и рефлексивной функции в информационном мире современного общества.

---

[1] Филина О. А. Проблемы современной информационной этики: автореф. дис. … канд. филос. наук. Тула. 2009.

[2] Черепанова М. В. Актуализация этических кодексов в контексте современной культуры // Известия ТПУ. 2013. Т. 322, № 6. С. 95.

[3] Там же.

При этом выявлено кроме преимуществ действующих кодексов этического поведения их недостатки, связанные с присущей им ограниченностью и расплывчатостью, что говорит еще раз о важности дальнейшего изучения этических кодексов и необходимости воспитания нравственных принципов в сознании социального субъекта, коллектива, общества. В связи с указанными замечаниями придание этическим кодексам следующих важных характерных особенностей позволит решить проблему повышения эффективности принятых моральных норм: 1) прагматичность, отражающаяся в четких принципах и установках; 2) диалог профессионалов и всех заинтересованных лиц в процессе формулирования моральных обязательств, составляющих этический свод правил; 3) содержание, укрепляющее и воплощающее в действительность правовые нормы и фундаментальные принципы.

Прикладной характер информационной этики находит отражение в регулирующих инвариантных моральных установках этических кодексов информационного общества. В роли критериев оценки человеческих поступков выступают универсальные этические представления, заложенные в базисе нравственных постулатов. В свою очередь, уровень социального субъекта, определяющий самосознание, отношение общества к нравственным проблемам, степень социальных санкций на нарушения моральных норм, задает эффективность применения принятых правил социального взаимодействия в информационной среде. В результате возникает потребность в дальнейшем усовершенствовании этических кодексов и исследовании функций информационной этики, как основообразующей социального феномена – информационная безопасность.

Подведем итог. Государственное управление информационной средой нами рассматривается как объект морально-правового регулирования, суть которого состоит в упорядочении управленческих отношений общества, основанных на

применении информационных технологий. Содержание этого координирующего механизма заключается в следующем:

- выработке и принятии новых правовых норм, соответствующих потребностями государства и современного общества в целом (правовое регулирование глобального пространства, гармонизация национального законодательства и международного права в информационной среде и т. д.);

- закреплении и упорядочении посредством моральных и правовых норм наиболее целесообразных общественных отношений в области государственного управления информационной среды (тайна данных, интеллектуальная собственность и т. д.);

- охране регламентированных правом управленческих отношений в процессе применения информационных технологий (включая назначение санкций за их нарушение);

- урегулировании общественных отношений, возникающих в ходе объективного развития информационного общества (формулирование этических кодексов, формирование общественного мнения и т. д.).

В связи с беспрецедентным ростом возможностей и масштабного внедрения информационных технологий, современное общество, в целях успешного и бесперебойного функционирования цифровой среды, нуждается в оперативном решении вопросов нормативного регулирования посредством выработки эффективных правовых норм. Правоприменительная практика информационной безопасности, основывающаяся на регламентирующих документах (законах, актах, договорах), требует своего дальнейшего изучения и модернизации. Важным фактором указанного процесса является всестороннее исследование с учетом баланса технических, этических, культурных и других аспектов. В свою очередь, технологии саморегуляции современного общества в виде кодексов этического поведения обязаны слаженно дополнить и усовершенствовать координирующий механизм норматив-

ного регулирования информационного пространства. Координирующий механизм морально-правовых норм должен закрепить в общественном сознании комплекс обязанностей и прав, внушить чувство ответственности и уважения к заданным социальным нормам.

Мы убеждены в том, что современное общество в рамках принятой модели информационной безопасности нуждается в выработке государственной социальной стратегии применения информационных технологий. Данная стратегия будет отвечать за выявление основных приоритетов общественного развития и формирование координирующего механизма социальных норм.

3.3. СИСТЕМА СОЦИАЛЬНОГО РЕГУЛИРОВАНИЯ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Сегодня информационная безопасность выступает как важное и необходимое условие безопасного существования всего мирового сообщества. Основной особенностью ее содержания становится закономерная тенденция роста значения гуманистической направленности, которая в первую очередь позволит нейтрализовать основные опасности и угрозы информационного характера, обеспечивая безопасное использование информационных технологий в современном обществе.

Решение рассматриваемого вопроса требует предварительных усилий с целью формирования безопасного существования в информационной среде. Анализ возможностей технологий завтрашнего дня, рассматриваемый в параграфе 4.1, показывает, что используемые обществом информационные технологии должны получать социальное содержание и воплощать цели, исключающие антигуманистическое применение. Разработка и внедрение новых информационных технологий, имеющих социально-гуманистическую направ-

ленность, определяются не только стараниями создателей технологий, но прежде самого общества, формирующего благоприятную гуманистически направленную социальную среду.

В данном русле особенную значимость приобретает оценка информационно-технических изобретений и перспектив использования информационных технологий, влияющих на выживание общества. Возможность обладать достоверной информацией о последствиях применения информационных технологий способствует предупреждению негативных проявлений различного характера. Неполная или недостоверная информация, незнание или непонимание последствий является глубинной причиной основного числа катастроф и аварий в будущем. Иначе гипотетическое будущее человечества обязано быть определяющим ориентиром развития возможных направлений системы информационных технологий. От того смещение приоритетов в содержании информационной безопасности сегодня неизбежно внесет изменения в структуру функционирования глобальной безопасности в поддержку общечеловеческих интересов.

Так, в рамках задачи защиты основных прав и фундаментальных свобод человека выполнение первого из двух выделенных условий в параграфе 4.1 – обеспечение максимального разнообразия легитимного контента в информационных сетях – предполагает удовлетворение в первую очередь тех информационных потребностей, которые способствуют прогрессу человечества. При этом в вопросе о рациональной информационной технологии, запрограммированной на уважение к человеческим ценностям, имеется в виду, что овладение обществом знанием и информацией посредством технологических средств будет направленно только на прогрессивное развитие.

В свою очередь, выполнение второго условия, заключающегося в обеспечении всеобщего доступа к информации и

информационным технологиям, предполагает расширение масштаба социальной базы информационной безопасности, что приведет к углублению государственного, общественного и личностного уровней функционирования. Гражданское общество, принимая обязательства по обеспечению всех категорий своего населения равными возможностями, в том числе и участия в информационном взаимодействии, без сомнений, заинтересовано в расширении масштабов социальной базы информационной безопасности.

На практике процесс роста социальной базы предполагает параллельное увеличение числа субъектов информационной безопасности. В результате проявляется важная задача, заключающаяся в повышении уровня образования и информационной культуры социальных субъектов и общества в целом. Данный вопрос охватывает как профессиональную деятельность в области информационных технологий, так и в равной степени любую деятельность в информационной среде, объединяющую всех субъектов информационных отношений. Поскольку именно уровень развития человеческих ресурсов в качестве основной предпосылки формирования научного, социального, экономического, культурного и духовного потенциала в конечном итоге определяет безопасность социума. В свете указанных перспектив наука и образование выступают решающими факторами обеспечения информационной безопасности как основной составляющей национальной безопасности.

Тенденция возрастания значения социальной составляющей информационной безопасности ведет к пониманию необходимости введения качественно новой формы защиты – социальных мер обеспечения информационной безопасности. Особая новизна подобной формы защиты обусловлена многоуровневой системой механизмов и форм поведения, совокупность которых обязана обеспечить информационную безопасность личности, общества, государства.

Для решения проблем информационной безопасности, на наш взгляд, необходима система мер, включающая меры воспитательного, образовательного характера, популяризацию и пропаганду в общественном сознании посредством всех возможных средств массовой информации и с применением всех современных информационных технологий, при активном участии государства, моделей, способов нравственного поведения в глобальном информационном пространстве и, что наиболее важно, проведением научных исследований в рамках становящейся отрасли этического знания, информационной этики.

Опишем основные уровни социальных мер информационной безопасности и направления функционирования защиты, дающие представление об их системном характере. Согласно нашей точке зрения, необходимо выделить три уровня организации социальных мер обеспечения информационной безопасности:

1) в масштабах всего общества (макроуровень);

2) в рамках организаций и социальных групп (мезоуровень);

3) на индивидуальном (микроуровень).

Перечисленные уровни социальных мер информационной безопасности задают, соответственно, и основные направления развития и функционирования обеспечения защиты.

На уровне общества в целом или макроуровне социальные меры информационной безопасности реализуются благодаря организации и регулированию информационных потоков, а также распространению средств, способов и своеобразных «алгоритмов» оценки, обработки информации и применению информационных технологий в процессе социального взаимодействия от массовой коммуникации до межличностного общения. На данном уровне субъектами защиты информационной безопасности выступают общество и госу-

дарство посредством деятельности конкретных социальных институтов, включающих систему распространения социальных норм, традиций, социокультурных ценностей, систему образования, формирования благоприятной социальной атмосферы, систему нравственного, правового регулирования и т. д.

На мезоуровне социальные меры защиты реализуются благодаря использованию и распространению информационных источников и специфических способов социального взаимодействия, оценки и переработки информации, характерных для конкретных организаций и социальных групп. Здесь можно выделить принятые в различных социальных группах или профессиональных организациях этические нормы, правила, регламентации, процедуры информационного взаимодействия и безопасного использования информационных технологий. К данному уровню относятся такие субъекты защиты, как социальные группы, производственные структуры, политические, общественные, религиозные и иные организации и объединения.

На микро- или индивидуальном уровне социальные меры обеспечения информационной безопасности осуществляются в процессе обучения и развития индивида посредством создания специфической регулятивной системы или комплекса механизмов и алгоритмов, определяющих поведение субъекта в информационной среде.

Определив структуру и содержание системы социальных мер обеспечения информационной безопасности, рассмотрим подробнее предусмотренные ею технологии защиты.

Так, в рамках государственной политики на макроуровне социальных мер обеспечения информационной безопасности необходимо предпринять следующие шаги:

1) разработать согласованную концепцию правового обеспечения информационной безопасности;

2) внедрить практику популяризации и пропаганды основных принципов информационной безопасности, прав и обязанностей в информационной сфере;

3) создать научно-методологическую базу в области информационной безопасности.

В исследовании социальных аспектов информационной безопасности И. Н. Букреев справедливо говорит, что проблемы информационной безопасности из своей специальной области давно перешли в область социальную, то есть область защиты прав человека и общества. При этом автор верно отмечает тот факт, что единственным гарантом их соблюдения здесь становится государство. Согласно его мнению, «эту функцию государство может реализовать через законодательство»[1].

Нами установлено, что наряду с усовершенствованием действующего законодательства в борьбе с преступлениями, совершаемыми при помощи компьютерных технологий, с целью защиты прав человека и общества необходима унификация национального законодательства и объединение усилий международного сообщества в выработке единых подходов в вопросах регулирования мирового информационного пространства. Важным фактором указанного процесса является всестороннее исследование проблем в данной сфере с учетом баланса технических, этических, культурных и других аспектов.

Далее в рамках осуществления государственной политики обеспечения информационной безопасности необходимо направить возможности средств массовой информации и функции системы образования на пропаганду и популяризацию в массовом сознании моделей и способов нравственного поведения в глобальном информационном пространстве, в

[1] Букреев И. Н. Социальные аспекты информационной безопасности // Информационное общество. 1998. Вып. 6. С. 44.

итоге формирующего основу системы информационной безопасности.

Изучая влияние информационных технологий на ценности человека, Т. Байнам определяет своеобразные ступени популяризации этического знания, способствующие решению проблем применения технологий современного общества[1]. Основные идеи указанной теории мы поддерживаем и в нашей работе по изучению проблем информационной безопасности.

В трудах Н. Винера, методологическая нить которых проходит через всю историю информационной этики, решаются фундаментальные задачи: защита главных человеческих ценностей, таких как жизнь, здоровье, безопасность, свобода, знание и использование новых возможностей. Основываясь на подобном подходе, необходимо изучение возникающих проблем в свете применения информационных технологий на двух различных ступенях, первая из которых базисная. Она важна тем, что дает прочувствовать всем представителям общественной системы тот факт, что процесс использования информационных технологий имеет социальные и этические последствия. Основные действия на данном уровне предполагают информирование широких масс населения о проблемах, возникающих в сфере создания и применения информационных технологий с целью их популяризации и пропаганды.

Средства массовой информации становятся одними из главных действующих лиц базисной ступени информационной этики. По мере того как растет влияние информационной технологии, система распространения информации и социокультурных ценностей обязана информировать о проблемах информационной безопасности, правах и обязанностях граж-

[1] Bynum T. The Development of Computer Ethics as a Philosophical Field of Study // The Australian Journal of Professional and Applied Ethics. 1999. № 1(1).

данина в данной сфере. Широкие слои общественности должны явно ощутить тот факт, что информационная технология может, как причинять вред ценностям человека, так и продвигать их.

На наш взгляд, максимальный эффект от усилий, прилагаемых на данной ступени популяризации знаний из области информационной безопасности и информационной этики, будет выражаться в увеличении количества социальных субъектов, которые, не являясь профессионалами в сфере информационных технологий, философии, юриспруденции или социологии, приобретут способность осуществлять предварительные оценки поведения субъектов общественных отношений в информационной среде, выявлять и идентифицировать возникающие социальные и этические проблемы.

Следующая ступень – «теоретическая» информационная этика, которая на заданном уровне призвана применять научные теории к анализу социальных и этических проблем, возникающих в обществе в процессе применения информационных технологий. Мы убеждены в том, что «теоретическая» информационная этика должна преподаваться в высших учебных заведениях, поскольку позволяет рассматривать специалисту возникающие этические ситуации, используя теории и инструменты из области философии, социологии и права с целью научного исследования и более детального анализа возникающих вопросов.

В действительности ни одна из этих ступеней популяризации этического знания не имеет четких границ, но все перечисленные «уровни анализа» необходимы для достижения главной цели – продвижения и защиты человеческих ценностей. Общество в лице каждого социального субъекта должно быть более восприимчиво ко всем возможным последствиям использования информационной технологии. Специалисты, работающие в сфере информационных технологий,

общественные деятели и политики, для повышения эффективности результатов своей деятельности обязаны иметь навыки и знания, как минимум предполагаемые на второй ступени. В свою очередь, представители научной среды обязаны продолжать углублять понимание социального и этического влияния вычислительной техники, занимаясь теоретическими анализами и исследованиями.

Государственная политика обеспечения информационной безопасности обязана включить в качестве одного их приоритетных направлений своей деятельности организацию и поддержку научных исследований в области разработки и внедрения информационных технологий, а также анализа и прогноза результатов ее использования. На наш взгляд, главной целью данных исследований, основанных на принципах информационной этики, прежде всего, должны стать обобщение опыта, формирование моделей и теоретических концепций, формулирование рекомендаций для реализации оптимальной системы информационной безопасности, прогнозирование и нейтрализация возможных негативных эффектов применения информационных технологий.

Кроме того, важным аспектом третьего условия (разработка научно-методологической базы в области информационной безопасности) является создание педагогических технологий относительно изучения проблем информационной безопасности и формирования информационной культуры в процессе обучения в системе образования. Обеспечение разработки и распространения научных, научно-популярных, учебно-методических материалов и литературы по проблемам информационной безопасности, информационной этики и информационной культуры общества. Осуществление подготовки и повышения квалификации педагогических кадров в целях организации учебного процесса на высоком профессиональном уровне в системе вузовского, школьного образования, профессиональной подготовки специалистов, способ-

ствующих формированию эффективной системы информационной безопасности.

В свою очередь, роль государства в обеспечении указанных процессов определяется отнюдь не жестким контролем каждого этапа или сферы информационного взаимодействия, она скорее носит особый вспомогательный характер, оттого мы назовем ее «бдительной опекой». Основные функции государства должны быть сосредоточены на следующих действиях:

- провозглашать и переводить на язык права этические принципы, лежащие в основе информационного общества;
- отслеживать и контролировать их эффективное осуществление;
- в случае необходимости, при обнаружении злоупотреблений или отсутствия поддержки провозглашенных ценностей субъектами различной деятельности, принять меры регулирования на основе методов прозрачности и открытости[1].

Сверх того, к функциям государства относится обязанность в качестве образца этического применения информационных технологий внушить уважение к принятым нормам нравственного регулирования и воплощать их в жизнь. Информационная этика обязана привести социум к осознанию принципов, на которых в дальнейшем необходимо строить информационное общество. В то же время, указанные принципы должны найти экстраполяцию в утверждении прав, которые отстаивают.

Формирование высоконравственной информационной среды – путь, проложенный далеко не на принуждении, через блокирование или наказание неугодных и несоблюдающих

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный центр библиотечного содружества. 2009. С. 18.

принятые правила. Прежде всего, это формирование воспитательных моделей, внедрение средств и разработка методов, предназначенных для усвоения людьми этических ценностей, воспитание уважения к ним и рефлексии. Ожидаемым результатом от указанных действий должны стать этическое саморегулирование в информационной среде, самоконтроль, основанный на ценностях солидарности и социальной ответственности.

Мезоуровень социальных мер обеспечения информационной безопасности включает формирование и внедрение защитных механизмов на коллективном уровне, основывающихся на идентификации индивида с конкретной социальной группой, общностью, объединением. Основной целью действия указанных механизмов является умение человека руководствоваться в процессе применения информационных технологий или информационного взаимодействия определенными оценками, нормами, мнениями, принятыми в социальной группе или профессиональной среде.

Выделим категории социальных групп и коллективов в области применения информационных технологий, испытывающих на сегодняшний день потребность в моральном регулировании социального взаимодействия в информационной среде.

1. Первую группу составляют специалисты, для которых информационные технологии являются областью профессиональной деятельности, включая виртуальных преподавателей, библиотекарей и коллективы, имеющие в информационной среде различного рода деловые, коммерческие отношения.

2. Вторая группа объединяет все категории пользователей и сообществ пользователей.

3. Третья группа представлена средствами массовой информации.

4. В четвертой группе представлены регулировщики контента в информационном пространстве Интернет, для которых этические кодексы, из-за отсутствия правовых рычагов деятельности, призваны служить обеспечением прозрачности в работе поисковых служб.

Профессиональная среда специалистов, работающих в области информационных технологий, уже достаточно продолжительное время занимается вопросами морального регулирования действий профессионалов в своей области. Например, этический кодекс ACM (Ассоциации производителей вычислительной техники)[1], принятый в 1992 году, этический кодекс IEEE (Институт инженеров электротехники и радиоэлектроники)[2], принятый в 1990 году. Перечисленные проекты сыграли существенную роль в деле привлечения внимания к профессиональной ответственности и продвижению идей повышения профессионализма и этического созревания компьютерных профессионалов. Содержащиеся в них заповеди доказывают, что специалисты не только опираются на принятые в обществе моральные нормы, но и соблюдают принципы информационной безопасности: тайна, конфиденциальность, точность и доступность информации.

Со своей стороны отметим, что сегодня вопрос профессиональной ответственности специалистов становится все более и более актуальным. Это обстоятельство определено повышением требований к уровню профессионалов, что связано с разворачивающейся обстановкой в области информационной безопасности и развитием информационного общества в целом. В свое время Р. Броди ввел понятие «информа-

[1] Gotterbarn D., Miller K., Rogerson S. Software Engineering Code of Ethics // Information Society. 1997. № 40 (11).

[2] Huff C., Martin D. Computing Consequences: A Framework for Teaching Ethical Computing // Communications of the ACM. 1995. № 38(12).

ционная наивность»[1] у профессионалов в области информационных технологий, проводя фундаментальное различие между смыслом слов «знать о» и «знать». Определение «информационной наивности» заключается в «состоянии, которое не может быть больше, чем реализация процесса, связанного с производством артефактов»[2]. Выходя за рамки принятого понимания наивности, то есть не более чем невежество или небрежность в обращении, привлечем под определение такие характеристики, как низкий уровень компетентности и недостаток в профессиональных знаниях.

На наш взгляд, в борьбе с подобным состоянием «информационной наивности» необходимо активнее использовать этические кодексы в индустрии производства информации и информационной технологии, которые обязаны требовать высокой профессиональной компетентности, точности, и предупредить проявления возможных негативных эффектов.

Таким образом, для специалистов профессиональный кодекс – своеобразный механизм социализации, главной задачей которого является информирование о действующих этических стандартах данной области. Оформленная коллективная мудрость лиц, представляющих профессию – основная функция кодекса этики[3]. По нашему мнению, профессиональные этические кодексы рассматриваемых категорий должны содержать не только специфические нравственные нормы поведения, обусловленные профессиональной деятельностью (защита конфиденциальной информации, совершенствование профессионального образа и т. д.), но и общечеловеческие моральные нормы (например, пиетет в области свободы и достоинства человека). В итоге кодекс этики от-

[1] Brody R. Information ethics in the design and use of metal // IEEE Technology and Society Magazine. 2003. Vol. 22(2). P. 34.
[2] Там же.
[3] Johnson. D. G. Computer Ethics. New Jersey: Prentice Hall, 2001.

ражает плоды многолетнего опыта, то, что представители профессии сочли наиболее важным, то, что необходимо помнить и воплощать в своей работе. Иначе говоря, согласованное олицетворение опыта большинства представителей профессии.

В то же время, проблемы в области использования информационных технологий не ограничиваются вопросами только в сфере профессионалов. Глобальная информационная сеть, благодаря своей универсальной среде и простоте технического использования, послужила почвой для образования различных социальных и культурных граней, позиционирующих себя в качестве отдельных субкультур, имеющих в арсенале свою систему ценностей и нормы поведения. Определенный уровень развития таких интернет-сообществ служит поводом для формулирования указанных атрибутов в кодексы и правила этического регулирования действий членов сформировавшихся групп (хакеры, блогеры и т. д.).

В свою очередь, этические кодексы конкретных сообществ интернет-пространства служат частными примерами решения этических проблем поведения в глобальной информационной сети посредством принятия определенных правил. В качестве более масштабного решения нивелирования указанных проблем исследователи предлагают выделить основные слагаемые Сетевой этики[1]: Кодекс Сетевой этики (регулятор отношений в Сети) и Сетевой этикет (регулятор поведения в Сети). В постулатах кодекса декларируются традиционные ценности, которые экстраполируются на взаимоотношения пользователей сети Интернет. Их цель – помочь человеку сохранить в себе человеческие качества, не потерять свое личностное начало, свою индивидуальную специфику в среде Интернет.

[1] Езова С. А. Слагаемые библиотечной этики // Библиосфера. 2010. № 2.

Относительно третьей группы пользователей, нуждающихся в регулировании деятельности этическими кодексами, отметим следующее. Профессиональная этика работников, представляющих средства массовой информации, имеет давнюю историю, связанную со становлением демократического, гражданского общества. С течением времени моральные правила, признаваемые всеми работниками медиасферы, сформировались в солидные этические каноны. Сегодня принципы международной журналистской этики сфокусированы на профессиональной честности и объективности, уважении к частной жизни и достоинству, отражении общественных интересов, всеобщих ценностей и многообразия культур, продвижении правды, соблюдении норм информационной безопасности, а так же личное убеждение воплощать в жизнь указанные принципы вопреки всякой корысти.

Высокие моральные нормы этического кодекса работники медиасферы, печатных СМИ, радио, телевидения, государственного вещания вместе с результатами своей деятельности обязаны проецировать из обычного мира в глобальные информационные сети. Сегодня, в период небывалого роста информационно-коммуникационных технологий, когда информационные источники оказывают воздействие на все сферы жизнедеятельности человека, средства массовой информации приобретают практически неограниченные возможности влияния на общественное настроение, поэтому как никогда важно помнить и воплощать в жизнь перечисленные выше нравственные постулаты.

Заключительная группа, требующая обязательного введения этических кодексов, составляет сообщество регулировщиков контента в информационном пространстве Интернет, поскольку, как упоминалось ранее, из-за отсутствия правовых рычагов подобной деятельности этические кодексы должны служить обеспечением прозрачности в работе поисковых служб.

Мы убеждены, что круг основных вопросов относительно контроля работы поисковых служб должен быть следующим: Кому подотчетны поисковые службы? Какие есть гарантии этичной деятельности этих компаний? Какими критериями руководствуются службы в процессах блокировки и распространения информационного контента? В связи с этим необходимо отметить такой инцидент: «Компания Google признала, что ее автомобили, проводя панорамную съемку улиц для картографического сервиса Street View, действительно нарушали неприкосновенность частной жизни. «Гугломобили», фотографируя города, параллельно собирали персональные данные граждан по незашифрованным сетям Wi-Fi на протяжении нескольких лет. Эта информация включала в себя логины, пароли, письма электронной почты. В подобных нарушениях также была уличена компания «Яндекс»[1]. Кроме того, на наш взгляд, к вопросам ответственности интернет-провайдера необходимо добавить такой аспект, как передача незаконного, запрещенного, опасного или неэтичного контента в интернет-среде. Так, сложившаяся ситуация наглядно показывает острую необходимость обсуждения этического кодекса для информационных посредников, которые обязаны информировать о принципах и методах, используемых в работе, гарантировать конфиденциальность информации, доверенной им.

Например, Европейская ассоциация по информационным услугам (EUSIDIC)[2] предлагает кодекс практики для производителей баз и банков данных. В пунктах этического кодекса производителей информационных ресурсов четко прослеживается направленность на соблюдение принципов инфор-

[1] Редикульцев С. Google и «Яндекс» заглядывают в личную информацию пользователей [Электронный ресурс]. – URL: http://www.vesti.ru/news (дата обращения: 14.03.2013).

[2] EUSIDIC. Официальный сайт [Электронный ресурс]. – URL: http://www.eusidic.org (дата обращения: 09.04.2014).

мационной безопасности: полноты, конфиденциальности и доступности. Этические правила направлены на сохранение должного уровня открытости информационных потоков, в то же время с учетом защиты персональных данных, а также обеспечения законных интересов всех сторон, участвующих в процессе производства, хранения и распределения информации. На наш взгляд, такие категории, как открытость, конфиденциальность, точность и справедливость являются основой фундамента в области профессиональной деятельности информационных посредников.

Кроме того, в рамках рассматриваемого вопроса о возможном регулировании указанной выше категории необходимо привлечь внимание заинтересованной общественности и ученых к этическим аспектам работы серверов диалоговых и азартных игр. По нашему мнению, введение определенных правил в предоставление услуг среды Интернет, должно способствовать снижению общего числа случаев развития психосоциальных расстройств, а значит в итоге защите детей и подростков.

Согласно Конвенции о правах человека[1], регулирование свободы слова и свободы доступа к информации в демократическом обществе связано с обязанностями и ответственностью. Сегодня вопрос заключается в определении механизмов и рычагов данного регулирования. Применить в сети уже существующие нормы в обществе или разработать особый регламентирующий документ для интернет-среды? Неприемлемые и незаконные формы информации в реальном мире являются настолько же недопустимыми в информационных сетях, или, возможно, виртуальная среда обусловливает существование особых форм выражения мнений, которые требуют особого контроля? Приемлемо ли в подобных случаях

[1] Конвенция о правах человека. Ст. 10, § 2 [Электронный ресурс]. – URL: http://www.conventions.ru/view_base.php?id=395 (дата обращения: 26.05.2014).

толерантное отношение к некоторым формам сетевого общения, недопустимое до сего момента в реальном мире? Ответы, по нашему мнению, призвана найти информационная этика, в том числе и за счет нормативного регулирования функций интернет-провайдеров, поскольку их деятельность решением ЕС не попадает под ответственность перед законом. Указанные случаи – лишь некоторые из череды претензий к работе регулировщиков контента в информационных сетях. С нашей точки зрения, процессам доступа и фильтрации информационного контента в работе информационных посредников необходимо придать большую прозрачность, как и разработать дополнительные гарантии в ее обеспечении.

Прав Т. Фрелих, выделяя самоконтроль в качестве способа эффективного регулирования информационного взаимодействия[1]. В этом ключе, необходимо отметить, и технические приемы его реализации: использование программ фильтрации, применение функций модераторов, разработку технических регламентов как программное обеспечение для фильтрации и рейтинговых процедур. В практике сегодняшнего дня существуют пока немногочисленные примеры активности конечных пользователей в процессах саморегулирования и совместного регулирования. Образцом совместного регулирования контента в интернет-среде может служить Википедия (англ. Wikipedia) – свободная общедоступная мультиязычная универсальная интернет-энциклопедия, занимающаяся привлечением всего гражданского информационного сообщества в процессы создания контента, редактирования и проверки фактов. В силу объективных причин данная энциклопедия не может составлять число научных

[1] Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. Munich: G. K. Saur, 1997.

изданий, в то же время она является одним из популярнейших информационных источников у пользователей сети Интернет.

Интернет-ресурс имеет собственный свод официальных правил[1], регулирующих отношения между разработчиками ресурса, авторами информационных сообщений и пользователями, интересующимися результатами общего труда. Указанные правила несут следующий смысл: между участниками взаимодействия утверждены принципы этичного поведения, не допускающие оскорблений, угроз и агрессии, актов вандализма и «многоликости» авторов. Оговаривается обязательность сохранения нейтралитета точки зрения автора, наличие ссылок на источники и недопустимость оригинальных исследований в сообщениях. «Соблюдение порядка» Википедия добивается путем достижения консенсуса через вежливое обсуждение и переговоры, а также не допускает ни при каких условиях использование анонимных прокси-серверов. В «Правовых основах» списка отражены условия, не позволяющие привести к нарушению чьих-либо авторских прав. Таким образом, подход, реализованный Википедией, демонстрирует доверительные отношения между членами информационного сообщества и повышение информированности об этических нормах.

Технические примеры процесса саморегулирования также нашли свое отражение в действующем проекте Internet Content Generated (Создание интернет-контента), предполагающем формирование особой среды Internet Democracy Generated (Создание демократической интернет-среды). Указанная среда позволяет гражданам обсуждать модели распространения, создания и развития информации в качестве

[1] Википедия: Список правил [Электронный ресурс]. – URL: http://ru.wikipedia.org (дата обращения: 19.02.2014).

«альтернативных механизмов управления» [1] в Интернете. Так, модель «Creative Commons»[2] или другие стихийно формирующиеся платформы позволяют производить мониторинг в интернет-среде на предмет нарушения этических и правовых норм.

Мы заключаем, что организация социальных мер на мезоуровне должна применять средства и методы формирования соответствующего социального климата и атмосферы корпоративности; обеспечить условия для идентификации личности с конкретным социальным коллективом и актуализации чувства принадлежности к определенной социальной организации; подготовить авторитетные внутригрупповые этические, профессиональные нормы или предписания к действиям, определяющие условия безопасного применения информационных технологий и функционирования в информационной среде.

Информационная этика, выполняя свою нравственно-регулятивную функцию, наряду с традиционно принятой моралью и правом, является механизмом, реализующим формирование нравственной среды в информационном пространстве современного общества, включая и информационное пространство отдельно взятого коллектива.

Этический кодекс обязан представлять собой специфический аттрактор, воплощающий некое итоговое развитие системы, состояние, которое она стремится достичь[3]. Так, в результате признания особой роли этического регулирования на групповом уровне обостряется потребность в изучении и

[1] Этика и права человека в информационном обществе: материалы европейской региональной конференции. М. : Межрегиональный цент библиотечного содружества. 2009. С. 17.

[2] Creative Commons [Электронный ресурс]. – URL: http://creativecommons.org (дата обращения: 18.02.2014).

[3] Филина О. А. Проблемы современной информационной этики: автореф. дис. … канд. филос. наук. Тула, 2009.

пропаганде принципов информационной этики, содействие ее институализации и усовершенствованию разработанных кодексов этического поведения в информационной сфере.

Сегодня процесс успешного функционирования системы информационной безопасности требует целенаправленной, последовательной работы, начинающейся с профессиональной ответственности и обсуждения этических и социальных последствий применения технологии еще в научно-исследовательской лаборатории на стадиях проектирования информационных технологий. Заключительное звено данной цепочки – конечный пользователь, обладающий ясным представлением об основах функционирования и использования конкретных информационных технологий. Успех указанного процесса, мы убеждены, кроется в определенных функциях сферы образования и бдительной опеки государства. В целях эффективного коммуникационного взаимодействия в информационной среде важно обеспечить необходимый уровень образованности и информированности пользователей о правах и обязанностях.

Л. Г. Сандакова, решая проблемы человека и его образования в информационном обществе, формулирует идею и обосновывает основные положения гуманитарной информационно-технологической парадигмы образования, в рамках которой устанавливается новая система социальных координат, новая система социальных норм, в первую очередь, этических, нравственных. Автор концепции четко определяет свою позицию, подчеркивая, что исходной точкой социально-гуманитарных наук является человек, причем во всех своих бытийных формах: от общества - до индивидуальности[1]. По этой причине оценка каждого состояния общества, каж-

[1] Сандакова Л. Г. Информационно-технологическая парадигма образования: гуманистическая сущность и концептуальные основы: автореф. дис. … д-ра филос. наук. Улан-Удэ. 2003.

дого социального движения обязана соотноситься с задачами совершенствования человека.

Основное содержание гуманитарной информационно-технологической парадигмы образования состоит в том, что целью развития общества является человек, т. е. его интеллектуальное, духовное, физическое и психическое развитие, определяющее потребности, интересы и смысл жизни. Новое мышление, характерное для человека информационной цивилизации, должно опираться не на познание, а на отношение, оно становится далеким от уровня созерцания, поскольку ориентировано на воплощение в «поступок»[1]. Таким образом, согласно данной концепции, образование, меняя индивидуальное сознание отдельного человека, трансформирует, в определенной степени, и общественное сознание. В результате основная ценность образования концентрируется в том, что оно – важнейший инструмент вступления общества в новое состояние, в котором строятся новые структуры и формы индивидуального и коллективного сознания.

Так, роль системы образования в информационном обществе отмечена особым значением в отношении не только обучения использованию информационных технологий, но и изучения гражданских и этических основ жизнедеятельности. Существенный вклад в реализацию задачи укоренения в сознании участников информационных отношений необходимости соблюдения норм информационной этики и воспитания навыков ее применения обязана внести система образования как социальный институт «создания социального человека»[2].

Такая задача, как информирование всех социальных субъектов об основах законодательства, правах, которыми

[1] Сандакова Л. Г. Философия образования: гуманитарная информационно-технологическая модель. М. : Спутник+, 2002.

[2] Субетто А. И. Сочинения. Ноосферизм: в 13 т. : Системология образования и образованиеведение. Кострома: КГУ им. Н. А. Некрасова. 2007.

они располагают, ограничениях, проблемах и возможностях с ними справиться в информационном мире, ложится на плечи системы образования. Одними из основных функций образования должны стать информирование и разъяснение правовых и этических аспектов обеспечения информационной безопасности на индивидуальном уровне в процессе обучения и развития личности.

С целью формирования здорового информационного общества образование обязано воспитывать у каждого индивида такие важные особенности, как осознание собственной роли в процессе обеспечения информационной безопасности, способность анализировать влияние технологий на социальную сферу и оценивать личные действия относительно ориентиров, заданных принятой системой нравственных ценностей. Что еще раз находит отражение в статьях «Этического кодекса для информационного общества» ЮНЕСКО[1]. Так, основой эффективного регулирования информационного взаимодействия должны стать правовое регулирование и самоконтроль.

Таким образом, индивидуальный или микроуровень социальных мер обеспечения информационной безопасности связан с формированием у индивида в процессе приобретения опыта использования информационных технологий и информационного взаимодействия (включая обучение с использованием специализированных форм подготовки, тренинговых занятий по определенным методикам) личностных образований, алгоритмов поведения, которые и образуют в своей совокупности индивидуальную систему этических установок, регулирующих его деятельность в информационной среде.

[1] Этический кодекс для информационного общества (проект) [Электронный ресурс]. – URL: http://www.osu.ru/docs/kodeks_ethics_info.doc (дата обращения: 30.08.2008).

Из рассмотренных направлений социальных мер обеспечения информационной безопасности, как правило, первые два уровня зависят от внешних условий и факторов, деятельности сторонних социальных субъектов, функционирования социальных институтов и т. д. Последнее направление зависит, в первую очередь, от самого индивида.

Формирование эффективной системы информационной безопасности и информационно-психологической безопасности личности зависит от того, насколько развито желание человека существовать в безопасной информационной среде, избежать информационных опасностей и угроз современного общества. Каждый индивид должен сам желать научиться обеспечивать информационную безопасность доступными ему средствами, то есть активность конечного субъекта предполагает, на наш взгляд, в первую очередь, знание собственных прав и обязанностей, а также воплощение в жизнь принципов информационной этики как основы обеспечения информационной безопасности.

В итоге социальные меры обеспечения информационной безопасности представляют собой многоуровневую систему технологий, принятую и поддерживаемую государством, обществом, коллективом, личностью, направленную на формирование особого регулятивного механизма, определяющего соответствующее нравственное поведение индивида в процессе применения информационных технологий и взаимодействия в информационной среде. Социальные меры еще раз утверждают и углубляют уже принятые морально-этические и правовые меры защиты информационной безопасности. Кроме того, социальные меры обеспечения информационной безопасности служат основанием для развития и популяризации в обществе формирующейся в рамках мировой науки общенаучной теории информационной безопасности. Они задают гуманистически ориентированное направление развития данной концепции, что в итоге приве-

дет к сдвигам в понимании сущности и специфики информационной безопасности.

Изменение видения человека в мире в конце XX веке позволило набрать вес аксиологической составляющей в системе глобальной безопасности. Суть подобного подхода заключается в следующем: всякая теория безопасности имеет возможность быть признанной в том случае, если она ориентирована на человека, согласована с его интересами, уважает информационные права и свободы. Теория современной безопасности значительно расширяет границы своего содержания. Экономические, социальные, психологические и другие аспекты придают ей гибкость и динамичность, способность отвечать требованиям конкретного исторического периода[1].

Сегодня достижения в исследовании фундаментальных проблем информационной безопасности формируют основные подходы к разработке общей теории информационной безопасности. Трудности ее создания объясняются, на наш взгляд, следующими причинами:

1. Комплексный характер описываемых проблем, интеграция различных наук.

2. Высокий процент субъективных факторов в области информационной безопасности.

3. Многообразие областей и причин возникновения информационных опасностей и угроз.

Общая теория информационной безопасности в конечном итоге должна представлять собой предметно и проблемно ориентированную научно-теоретическую конструкцию. В то же время важно отказаться от представлений о ней как об объединенной концепции, изучающей все разнообразие информационных опасностей и угроз, включающей все грани и стороны информационной безопасности, рассматриваемые различными науками. Указанные аспекты слишком разнооб-

[1] Белая книга российских спецслужб. М. : Обозреватель. 1999.

разны и многочисленны по своему характеру, в результате чего их искусственное объединение вряд ли представляется возможным.

Определяя место формирующейся общенаучной теории в системе научных знаний, необходимо обозначить ее взаимоотношения с другими специальными теориями безопасности, выяснить связь с общественными, техническими и естественными науками, поскольку, с нашей точки зрения, в каждой из научных областей рядом с другими проблемами косвенно или прямо решаются вопросы информационной безопасности. В результате чего можно говорить о том, что общенаучная теория информационной безопасности имеет связь с каждой областью знаний, методологически поддерживая все исследования по решаемой проблематике. Важно отметить, что речь идет об универсальном целом, раскрывающем принципы обеспечения информационной безопасности в различных областях действительности.

Согласно своему теоретическому статусу, формирующаяся теория определяется как отдельное направление исследований, ориентированное на изучение комплексных пограничных проблем, что роднит ее с аналогичными теоретическими направлениями. Общая теория информационной безопасности обеспечивает пересечение прикладных дисциплин, используя системную основу, что делает ее таким научным направлением, которое наиболее ярко передает целостность и единство мироздания, условность дробления наук[1]. Следовательно, изучаемая теория становится исходной точкой и методологической основой для дальнейшей выработки специализированных концепций информационной безопасности. В итоге общая теория информационной без-

[1] Захаров М. Ю. Информационная безопасность социума: социально-философское исследование: автореф. дис. … д-ра филос. наук. Ростов н/Дону, 1998.

опасности интегрирует прикладные аспекты наук для исследования содержания, сущности, методов и средств обеспечения информационной безопасности.

Общая теория информационной безопасности, наряду с принятыми стандартами, жестко регламентирующими структуру информационных технологий и информационной среды, должна включать и нетехнические подходы к оценке защиты информационных объектов, связывать в единую структуру все значимые с точки зрения безопасности элементы и факторы. Формирующаяся теория обязана определить место всех частей информационно-когнитивного целого в системе информационной безопасности.

Выделим основные задачи общенаучной теории информационной безопасности:

- классификация и обобщение научных знаний в области информационной безопасности;
- решение методологических проблем данной сферы;
- анализ и определение фундаментальных понятий дисциплины.

По нашему мнению, общая теория информационной безопасности, прежде всего, должна содержать мировоззренческие и методологические аспекты научной области. Потому как особую значимость в настоящее время приобретают проблемы защиты от информационных угроз и опасностей, возникающие в самом обществе, соответственно, конкретизацию и продолжение общей теории информационной безопасности обеспечат ее социально-философские основания.

Подведем итоги. Безопасное существование в информационной среде с минимальным уровнем риска возникновения информационных опасностей и угроз требует предварительных усилий. Тенденция возрастания значения социальной составляющей информационной безопасности приводит к пониманию необходимости введения качественно новой

формы защиты – социальных мер обеспечения информационной безопасности.

Для решения проблем информационной безопасности современного общества разработана система мер, включающая меры воспитательного, образовательного характера, популяризацию и пропаганду в общественном сознании посредством всех возможных средств массовой информации и с применением всех самых современных информационных технологий, при активном участии государства, моделей, способов нравственного поведения в глобальном информационном пространстве и, что наиболее важно, проведением научных исследований в рамках становящейся отрасли этического знания, информационной этики.

Новые меры защиты представляют многоуровневую систему механизмов и форм поведения, совокупность которых обязана обеспечить информационную безопасность: 1) в масштабах всего общества (макроуровень); 2) в рамках организаций и социальных групп (мезоуровень); 3) на индивидуальном (микроуровень).

В рамках макроуровня социальных мер обеспечения информационной безопасности основными субъектами защиты являются государство и общество. В целях обеспечения информационной безопасности указанных категорий субъектов безопасности программа государственной политики обязана: разработать согласованную концепцию правового обеспечения информационной безопасности; внедрить практику популяризации и пропаганды основных принципов информационной безопасности, прав и обязанностей в информационной сфере; создать научно-методологическую базу в области информационной безопасности.

К мезоуровню социальных мер обеспечения информационной безопасности относятся следующие субъекты защиты, такие как социальные группы, производственные структуры, политические, общественные, религиозные и иные организа-

ции и объединения. В качестве технологий защиты безопасности здесь выделены принятые в различных социальных группах или профессиональных организациях этические нормы, правила, регламентации, процедуры информационного взаимодействия и безопасного использования информационных технологий.

На микро- или индивидуальном уровне социальные меры обеспечения информационной безопасности осуществляются в процессе обучения и развития индивида с целью формирования в его сознании специфической регулятивной системы или комплекса механизмов и алгоритмов, определяющих поведение социального субъекта в информационной среде.

Таким образом, социальные меры обеспечения информационной безопасности представляют собой многоуровневую систему технологий, принятую и поддерживаемую государством, обществом, коллективом, личностью, направленную на формирование в общественном сознании особого регулятивного механизма, определяющего соответствующее нравственное поведение индивида в процессе применения информационных технологий и социальных отношений в информационной сфере.

Кроме того, работа определяет особенности развития, основные задачи и место в системе научного знания формирующейся общей теории информационной безопасности, связывающей в единую структуру все части информационно-когнитивного целого в системе информационной безопасности. Особая значимость процесса обеспечения защиты от информационных угроз и опасностей, возникающих в обществе, говорит о необходимости формирования социально-философских оснований общей теории информационной безопасности. В свою очередь социальные меры обеспечения безопасности послужат основанием для развития и популяризации в обществе социально-философской концепции информационной безопасности в рамках формирующейся ее общенаучной теории.

ЗАКЛЮЧЕНИЕ

На рубеже XX и XI веков человечество шагнуло на ступень кардинальных технологических преобразований, связанных с возникновением нового ряда значительных опасностей и угроз. Пройти путь по восходящей лестнице к новой информационной цивилизации, основанной на колоссальных возможностях технологий, не сорваться вниз, способно общество с высокими нравственными идеалами и ясным пониманием всей глубины ответственности за каждый свой шаг. Сегодня информационные технологии, рассматриваемые как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование информационной реальности, повлияли на сознание человека и его возможности, изменили жизнь общества, трансформировали приоритеты и ценности. Как эти высокие технологии, являясь средством осуществления жизнедеятельности человека, будут применены в будущем, зависит от общества и его выбора.

В свое время основатели концепции информационного общества справедливо отмечали, что информация и знания станут ключевым фактором развития, превосходящим по значимости все виды материального производства, энергии и услуг. В этой теории информационные технологии и телекоммуникации представлены основным агентом экономических, социальных и политических изменений в современном мире. Вместе с тем, прогнозы ближайшего будущего социального строя в сравнении с нынешними реалиями оказываются несколько утопическими. Концептуальный анализ позволил выявить относительно невысокую степень критичности исследователей к феномену информационного общества, в силу чего оказались слабо принятыми в расчет возникающие в современном социуме новые виды опасностей и угроз.

На общем фоне деформации системы ценностей информационная сфера оказалась сердцевиной экономических, со-

циальных, политических и других конфликтов в обществе. Из ряда информационных опасностей и угроз, систематизированных относительно сфер жизнедеятельности общества, выделим реальную угрозу «информационного расслоения», расцвет компьютерной преступности, потенциальную угрозу дегуманизации труда и реальную угрозу техностресса, производство новых видов информационного оружия, угрозу информационного колониализма, развитие различных видов заболеваний, угрозу манипулирования человеческим сознанием, ведущую к психической и социальной дезадаптации человека. Так перед человеком развернулись все масштабы проблем информационной безопасности – противоречие между предоставляемыми возможностями информационных технологий, с одной стороны, и негативными эффектами, опасностями, угрозами их применения в деструктивных целях по отношению к личности, обществу, государству – с другой. Вследствие этого обеспечение безопасности результатов использования информационных технологий, устранение информационных опасностей и угроз в рамках стратегии информационной безопасности становятся стратегической проблемой мирового сообщества.

В монографии информационная безопасность представлена как устойчивое состояние информационной сферы, обеспечивающее свою целостность и защиту объектов при наличии неблагоприятных внутренних и внешних воздействий на основе осознания социальными субъектами своих ценностей, потребностей (жизненно важных интересов) и целей развития. Основное содержание понятия «информационная безопасность» заключается в обеспечении безопасности информации, обеспечении безопасности субъектов информационного взаимодействия от негативного информационного воздействия, удовлетворении информационной потребности субъектов информационного взаимодействия посредством обеспечения безопасного состояния информаци-

онной среды. Аксиологический, гносеологический и онтологический аспекты раскрывают философское содержание рассматриваемого определения. Онтологический аспект информационной безопасности фиксирует ситуацию преодоления опасности, целью которой является обеспечение целостности объекта и устойчивого состояния информационной среды. Антропологический аспект понятия выявляет обеспечение безопасности субъекта информационного взаимодействия. Аксиологическая составляющая понятия «информационная безопасность» отражает ценности и цели, определяющие информационные потребности субъекта. В итоге выделенное основное системообразующее содержание информационной безопасности, определяет ее в качестве целостного социального феномена объективного развития современного социума, направленного на содействие гармоничному развитию информационного общества.

Как показало проведенное исследование, информационная безопасность охватывает следующие направления: обеспечение защиты информационного пространства, поддерживающего справедливое распределение своих благ и ресурсов; содействие процессу перехода к устойчивому развитию формирующейся общемировой информационной среды; обеспечение состояния защищенности культурного генофонда человечества в условиях глобализации. Действительно, на современном этапе развития общества эффективное обеспечение информационной безопасности позволяет решать ключевые вопросы практически всех видов национальной безопасности. Информационная безопасность является важной составляющей системы национальной безопасности, и от успешного разрешения вопросов данной области зависит обеспечение глобальной общемировой безопасности.

В свою очередь, процесс обеспечения информационной безопасности перманентный, комплексный, социально-культурные аспекты являются важными его компонентами

наряду с правовыми и организационно-техническими средствами и методами. Изучение особенностей функционирования основных мер информационной безопасности привело к выводу, что систему защиты безопасности невозможно построить основываясь исключительно на технических средствах, прежде всего, прочность системы безопасности определяется профессионализмом и личностными качествами каждого их членов коллектива, а повышение ее уровня происходит за счет законодательных и морально-этических мер. В процессе обеспечения информационной безопасности морально-этические принципы и ответственность каждого, основанные на принятых правилах поведения в обществе и подкрепленные мерами законодательного характера на государственном уровне выступают в качестве главного фактора построения системы защиты. Кроме того, мы констатируем, что на сегодняшний день существует острая необходимость в целенаправленном формировании информационной культуры общества, от которой во многом зависит успешное решение проблем и вызовов, возникающих в процессе становления планетарного информационного пространства, и, соответственно, проблем информационной безопасности в целом.

Таким образом, основание информационной безопасности составляет поведение социального субъекта, ясно осознающего свои права и обязанности. При этом система морально-этических норм выступает в качестве руководства безопасного применения информационных технологий и формирования общественных отношений в информационной сфере. Так, в свете обеспечения безопасности информационных технологий на первый план выходит информационная этика, которая направлена на информирование каждого социального субъекта о его правах и обязанностях в информационном обществе, от ответственности за создание и использование информационно-компьютерных технологий и иных форм информации.

В современном социальном пространстве, организованном информационной технологией, возникновение информационной этики не является чем-то неорганичным или случайным. Вехи ее становления неразделно связаны с развитием информационных технологий и социально-культурной трансформацией общества. В истории формирования информационной этики нами выделены три основных периода:

- первый этап связан с именем Н. Винера, который в середине 40-х годов XX века предсказал новые этические проблемы, грядущие вслед за внедрением электронных компьютеров;

- второй этап начинается с обоснования в 1976 году теории компьютерной этики в качестве отдельной философской дисциплины, изучающей этические проблемы в сфере использования компьютерной технологии;

- третий этап сводится к появлению непосредственно самого термина «информационная этика» в 1988 году, в период бурного развития глобальной коммуникационной сети Интернет.

Кроме того, современная информационная этика имеет свои этико-философские истоки. Теория информационной этики формировалась под влиянием этики добродетели Аристотеля, деонтологической концепции И. Канта и этики утилитаризма. Сегодня наследие этих принципов и представлений о моральном поведении, заложенное в систему постулатов этического анализа, позволяет наиболее эффективно оценить модели и методы информационного взаимодействия социальных субъектов.

В свою очередь, сложившиеся характеристики этики будущего информационного общества определяют ее в качестве онтоцентрической теории, стремящейся оценить с моральной точки зрения всю существующую в мире информацию, в первую очередь, о человеке и его общественных отношениях в информационной среде. Информационная этика

имеет глобальный характер и значение, поскольку ее универсальные инструменты и механизмы служат при решении социальных и этических проблем всех видов и отношений, они обязаны обеспечить гармоничное развитие человеческого общества на основе межкультурного диалога цивилизаций. Так, этико-философские истоки информационной этики и сформировавшиеся характеристики, позволяют определить методологию решения многих социальных и этических проблем информационного общества, вызванных влиянием масштабного применения технологических достижений во всех сферах жизнедеятельности и смещением системы ценностей.

Следующий вывод касается того, что информационная этика представляет собой сложную и самоорганизующуюся систему, обладающую иерархической структурой с характерными взаимосвязями ее компонентов. Основными ее разделами являются компьютерная этика и киберэтика, а также раздел вопросов моральной ответственности специалистов в области безопасного использования информационных технологий. При этом перечисленные компоненты системы необходимо рассматривать в виде подсистем, обладающих относительной самостоятельностью и содержащих в своей структуре собственные элементы. Задачи и особенности составляющих подсистем в конечном итоге и задают характер взаимодействия и функции частей системы в целом. Система информационной этики является открытой, функционирующей и развивающейся.

По нашему мнению, благодаря слаженной работе всех приведенных компонентов системы, согласно функциям каждого составляющего звена, информационная этика формирует нравственное сознание человека в своеобразный нормативный порядок знаний, регулирующий общественные отношения в информационной среде, тем самым обеспечивая решение поставленных задач информационной безопасности.

Информационная этика призвана повысить компетентность социальных субъектов об их правах и обязанностях в информационном обществе. В результате, бесспорно, роль информационной этики в процессе обеспечения информационной безопасности выходит на первый план. Кроме того, такие категории, как «безопасность» и «ответственность», преобразуются в методологические основания социальных норм, регулирующих деятельность человека в информационном обществе.

Решая проблемы обеспечения информационной безопасности, в значительной мере вызванные утратой гуманистических нравственных ценностей, идеалов и подчинением морали политико-идеологическим интересам, информационная этика формулирует свои принципы: принцип доступности, принцип полноты и целостности информации, принцип конфиденциальности и принцип ответственности. Указанные принципы информационной этики в целях достижения образцов нравственности, справедливости и защиты моральных ценностей в процессе применения информационных технологий и социальных отношений в информационной среде позволяют создать нравственную основу для обеспечения деятельности современного общества в сфере информационной безопасности.

Принципы информационной этики находят свое отражение в пунктах Декларации прав человека ООН, доказывая одну из важнейших задач информационной этики, содействующую развитию процесса гуманизации социума: основным приоритетом применения информационных технологий на службе обществу и государству являются защита прав и фундаментальных свобод человека. В целях достижения поставленной задачи определены два необходимых взаимодополняющих друг друга условия: обеспечение максимального разнообразия легитимного контента в информационных се-

тях и обеспечение всеобщего доступа к информации и информационным технологиям.

Высокая скорость новых решений в области информационных технологий оказывает самое непосредственное влияние на права и фундаментальные свободы человека, от того возникает настоятельная потребность учитывать последствия их применения благодаря анализу и программированию возможностей информационных технологий на уважение к человеческим ценностям. В этом ключе, информационная этика доказывает свою способность предвидеть и влиять на результаты использования информационно-коммуникационных технологий. Изучение перспектив использования новейших технологий позволяет прийти к выводу о том, что информационное общество обязано обеспечить в качестве одного их приоритетных направлений государственной политики организацию и поддержку научных исследований в области разработки и внедрения информационных технологий, а также всестороннего анализа и прогноза результатов ее использования. Используемые обществом информационные технологии должны получать социальное содержание и воплощать цели, исключающие антигуманистическое применение.

В монографии утверждается положение, что этические нормы в сфере информационной безопасности требуют всемерного поддержания, в том числе на государственном уровне, то есть путем принятия нормативных актов, кодексов, законов, обеспечивающих права и свободы человека в информационном обществе, а также разработанного четкого механизма их реализации, доступного каждому социальному субъекту. Уважать заданные правовые положения в условиях постоянного ужесточения внутренних и международных правовых требований к безопасности становится актуальнейшей задачей современного социума. В итоге, информационное общество в рамках принятой модели информационной

безопасности должно выработать государственную стратегию развития и применения информационных технологий, включающую выявление основных приоритетов социального развития и создание правовых координирующих механизмов. Важным фактором указанного процесса является всестороннее исследование с учетом баланса технических, этических, культурных и других аспектов.

В свою очередь, этические принципы, пропагандируемые в кодексах поведения современного общества, обязаны усовершенствовать правовое регулирование информационного пространства путем внедрения механизмов саморегуляции. В исследовании выделяется основная роль этических кодексов, концентрирующаяся на выполнении нравственно-регулятивной и рефлексивной функции в информационном мире современного общества. Определены основные категории социальных групп и коллективов информационного общества, испытывающие на сегодняшний день потребность в установленных моральных нормах, регулирующих социальное взаимодействие в информационной среде: профессионалы, для которых информационные технологии являются областью работы; все категории пользователей и сообществ пользователей; средства массовой информации; организации, ведущие в информационной среде различного рода деловые, коммерческие отношения; виртуальные преподаватели и библиотекари; регулировщики контента в информационном пространстве Интернет.

Кроме того, философско-этический анализ выявил кроме преимуществ действующих кодексов этического поведения их недостатки, связанные с присущей им ограниченностью и расплывчатостью, что говорит еще раз о важности дальнейшего изучения этических кодексов и необходимости воспитания нравственных принципов в сознании социального субъекта, коллектива, общества. В связи с указанными замечаниями придание этическим кодексам следующих важных

характерных особенностей позволит решить проблему повышения эффективности принятых моральных норм:

1) прагматичность, отражающаяся в четких принципах и установках;

2) диалог профессионалов и всех заинтересованных лиц в процессе формулирования моральных обязательств, составляющих этический свод правил;

3) содержание, укрепляющее и воплощающее в действительность правовые нормы и фундаментальные принципы.

Уровень социального субъекта, определяющий самосознание, отношение общества к нравственным проблемам, степень социальных санкций на нарушения моральных норм, задает эффективность применения принятых правил социального взаимодействия в информационной среде. В результате возникает потребность в дальнейшем усовершенствовании этических кодексов и исследовании функций информационной этики, как основообразующей социального феномена – информационная безопасность.

Таким образом, государственная стратегия обязана укоренить в общественном сознании уважение к заданным социальным нормам (моральным, правовым) путем соответствующего законодательства и этического регулирования, связанного с гармоничным развитием общественных отношений в информационной сфере. Тенденция возрастания значения социальной составляющей информационной безопасности ведет к пониманию необходимости введения новой формы защиты – социальных мер обеспечения информационной безопасности. Подобные меры защиты обусловлены многоуровневой системой механизмов и форм поведения, совокупность которых обеспечивает информационную безопасность личности, общества, государства.

В рамках макроуровня социальных мер обеспечения информационной безопасности, где основными субъектами защиты являются государство и общество, программа государ-

ственной политики обязана разработать согласованную концепцию правового обеспечения информационной безопасности; внедрить практику популяризации и пропаганды основных принципов информационной безопасности, прав и обязанностей в информационной сфере; создать научно-методологическую базу в области информационной безопасности. В качестве технологий защиты безопасности мезоуровня социальных мер обеспечения информационной безопасности, субъектами защиты которого являются социальные группы, профессиональные организации и иные объединения, выделены разработанные и принятые в данных организациях и группах этические нормы, кодексы, правила, регламентации, процедуры информационного взаимодействия и безопасного использования информационных технологий. На микро- или индивидуальном уровне социальные меры обеспечения информационной безопасности осуществляются в процессе обучения и развития индивида с целью формирования специфической регулятивной системы или комплекса механизмов и алгоритмов, определяющих поведение субъекта в информационной среде.

Так, социальные меры обеспечения информационной безопасности представляют собой многоуровневую систему технологий, принятую и поддерживаемую государством, обществом, коллективом, личностью, направленную на формирование в общественном сознании особого регулятивного механизма, определяющего соответствующее нравственное поведение индивида в процессе применения информационных технологий и социальных отношений в информационной сфере.

Кроме того, в монографии определены особенности развития, основные задачи и место в системе научного знания формирующейся общей теории информационной безопасности, обязанной связать в единую структуру все части информационно-когнитивного целого в системе информационной

безопасности. Особая значимость процесса обеспечения защиты от информационных угроз и опасностей, возникающих в обществе, говорит о необходимости формирования социально-философских оснований общей теории информационной безопасности. В свою очередь социальные меры обеспечения безопасности послужат основанием для развития и популяризации в обществе социально-философской концепции информационной безопасности в рамках формирующейся общенаучной теории информационной безопасности. На наш взгляд, социально-философские основания позволят обеспечить данной теории конкретизацию и развитие, задавая гуманистически ориентированное направление, что в итоге приведет к сдвигам в общественном сознании понимания сущности и специфики информационной безопасности.

Дальнейшее развитие рассматриваемой в диссертации проблематики может осуществляться в рамках исследований информационной безопасности, становления информационного пространства, формирования подходов к устойчивому развитию общества. Решение перечисленных проблем, несомненно, будет способствовать формулированию этических кодексов поведения социальных групп и коллективов, воспитанию информационной культуры, безопасному применению информационных технологий, переходу общества на новую модель безопасного развития цивилизации. Осуществление подобной стратегии выживания человечества нуждается в исследовании перспектив системно-футурологического характера и закономерностей социального развития, неотъемлемым атрибутом которого должна стать безопасная информационная технология.

ЛИТЕРАТУРА

1. Абдеев Р. Ф. Философия информационной цивилизации: Диалектика прогрессивной линии развития как гуманная общечеловеческая философия для XXI в. / Р. Ф. Абдеев. – Москва: ВЛАДОС, 1994. – 334 с. ISBN 5-87065-012-7 : Б. ц.

2. Абрамов Ю. Ф. Информационная цивилизация: природа и перспективы развития / Ю. Ф. Абрамов, О. В. Бондаренко, В. К. Душутин. – Иркутск: Редакционно-издательский отдел Иркутского государственного университета, 1998. – 97 с.

3. Абрамов Ю. Ф. Научная картина эколого-информационного общества (методология устойчивого развития) / Ю. Ф. Абрамов, О. В. Бондаренко, В. И. Куйбарь. – Иркутск : Изд-во Иркут. ун-та, 2004. – 64 с.

4. Алексеева И. Ю. Этика Интернет. Internet Ethics / И. Ю. Алексеева. – Edited by D. Langford. – Houndmills etc.: Macmillan press, 2000. – 281с. ISBN 0-333-77626-7.

5. Алексенцев А. И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» / А. И. Алексенцев // Безопасность информационных технологий. – 1999. – № 1. – С.16-20.

6. Анисимов С. Ф. Духовные ценности: производство и потребление / С. Ф. Анисимов. – Москва : Мысль, 1988. – 253 с. ISBN 5-244-00001-2 (В пер.).

7. Антопольский А. А. Ответственность за правонарушения при работе с конфиденциальной информацией / А. А. Антопольский // Административная ответственность. – Москва : ИГиП РАН, 2001. – С. 124-130.

8. Апресян Р. Г. Идея морали и базовые нормативно–этические программы / Р. Г. Апресян. – Москва : Институт философии, 1995. – 353 с. ISBN 5-201-01862-9 : Б. ц.

9. Аристотель. Большая этика. / Аристотель // Сочинения. – Москва: Мысль, 1984. – Т. 4. – С. 295-375.

10. Аристотель. Никомахова этика / Аристотель // Сочинения. – Москва: Мысль, 1984. – Т. 4. – С. 53-294.

11. Аристотель. О душе / Аристотель // Сочинения. – Москва : Мысль, 1984. – Т. 1. – С. 371-448.

12. Артамонова Я. С., Артамонов П. А. Информационная безопасность и информационные коммуникации // T-Comm - Телекоммуникации и транспорт. – 2012. – № 4. – С. 69-70.

13. Архангельский Л. М. Ценностные ориентации и нравственное развитие личности / Л. М. Архангельский. – Москва : Педагогика, 1987. – 64 с.

14. Асаул А. Н. Организация предпринимательской деятельности / А. Н. Асаул. – Санкт-Петербург: АНО ИПЭВ, 2009. – 336 с. ISBN 978-5-91460-023-2.

15. Астахова Л. В. Информационная безопасность: герменевтический подход / Л. В. Астахова. – Москва: РАН, 2010. – 185 с. ISBN: 978-5-904197-11-7.

16. Астахова Л. В. Информационная и психологическая безопасность в регионе: культурологический аспект / Л. В. Астахова // Безопасность в информационной сфере. – 2011. – № 2. – С. 40-47.

17. Атаманов Г. А. Информационная безопасность в современном Российском обществе (социально-философский аспект): автореф. дис. … канд. филос. наук / Г. А. Атаманов. – Волгоград, 2006. – 24 с.

18. Атаманов Г. А. Информационная безопасность: сущность и содержание / Г. А. Атаманов // Бизнес и безопасность в России. – 2007. – №7. – С. 104-109.

19. Атаманов Г. А. О необходимости философского обоснования проблемы информационной безопасности // Власть и воздействие на массовое сознание. – Пенза: РИО ПГСХА, 2007. – С. 84-87.

20. Афанасьев В. Г. Системность и общество / В. Г. Афанасьев. – Москва: Политиздат, 1980. – 368 с.

21. Бабкин С. А. Интеллектуальная собственность в Интернет / С. А. Бабкин. – Москва: Щит-М, 2006. – 94 с. ISBN 5-89158-070-5.

22. Бабурин С. Н. Стратегия национальной безопасности России. Теоретико-методологические аспекты / С. Н. Бабурин, А. Д. Урсул, М. И. Дэлиев. – Москва: Магистр, 2014. – 512 с. ISBN 978-5-9776-0224-2.

23. Беззубцев О. А. О лицензировании и сертификации в области защиты информации / О. А. Беззубцев, А. Н. Ковалев. [Электронный ресурс]. – URL: http://www.cryptopro.ru.

24. Бентам Дж. Введение в основания нравственности и законодательства / Дж. Бентам. – Москва: РОССПЭН, 1998. – 415 с.

25. Бакштановский В. И. Ойкумена прикладной этики: модели нового освоения / В. И. Бакштановский, Ю. В. Сагомонов. – Тюмень: НИИ ПЭ ТюмГНГУ, 2007. – 390 с. ISBN 978-5-88465-833-8.

26. Бакштановский В. И. Честная игра : Нравственная философия и этика предпринимательства / В. И. Бакштановский, Ю. В. Сагомонов. – Томск: Томск. ун-т, 1992. – 240 с.

27. Басов С. А. Принять нельзя отложить. О знаках препинания в проекте Кодекса библиотечной этики / С. А. Басов // Библиотечное дело. – 2011. - № 06 (144)11. – С. 36-41. ISBN: 1727-4893.

28. Бачило И. Л. Информационное право: основы практической информатики / И. Л. Бачило. – Москва: Юринформцентр, 2001. – 352 с. ISBN 5-89194-090-6.

29. Белая книга российских спецслужб. – Москва: Обозреватель, 1999. – 272 с. ISBN 5-86014-078-9 : Б. ц.

30. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования. Перевод с англ. / Д. Белл. – Москва: Academia, 1999. – 956 с. ISBN 5-87444-203-0 (в пер.)

31. Белл Д. Третья технологическая революция и ее возможные социоэкономические последствия / Белл Д. // Информационная революция: наука, экономика, технология. – Москва, 1992. – С. 27-34.

32. Белов Г. В. Парадигма Информационного общества и становление информационного права. Теория и практика общественно-научной информации / Г. В. Белов. – Москва, 2003. – Вып. 18. – С. 39-55.

33. Белякова Г. И. Профессиональная этика / Г. И. Белякова. – Москва: Знание, 1975. – 64 с.

34. Бердяев Н. А. Человек и машина / Н. А. Бердяев // Путь. – 1933, май. – С.12-24.

35. Благодатских В. А. Стандартизация разработки программных средств / В. А. Благодатских, В. А. Волнин, К. Ф. Поскака-

лов. – Москва: Финансы и статистика, 2006. – 283 с. ISBN 10:5-279-02657-3.

36. Бодрийяр Ж. Общество потребления / Ж. Бодрийяр. – Москва: Республика, 2006. – 272 с. ISBN 5-250-01894-7.

37. Большой энциклопедический словарь: В 2-х т. / гл. ред. А. М. Прохоров. – Москва: Сов. энциклопедия, 1991. – 14768 с.

38. Бондаренко С. В. Киберэтика и сетевые сообщества (молодежный аспект проблемы с точки зрения американских социологов и психологов) / С. В. Бондаренко // Социальные и психологические последствия применения информационных технологий. – Москва, 2001. – С. 243-252. ISBN 5-98554-094-5.

39. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. – 2013. – №1. – [Электронный ресурс]. – URL:http://s3r.ru/2013/12/voprosyi-iberbezopasnosti/sybersecurity_issues_2013_1

40. Бреннер Д. Л. Телекоммуникации и мировая информационная революция / Д. Л. Бреннер // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 35-38.

41. Букреев И. Н. Социальные аспекты информационной безопасности / И. Н. Букреев // Информационное общество. – 1998. – Вып. 6. – С. 42 - 45.

42. Ван Дюн Дж. Роль человеческого фактора в совершении преступлений в сфере компьютеров / Дж. Ван Дюн // Компьютеризация общества и человеческий фактор. – Москва, 1988. – С. 202-218.

43. Валла Л. Об истинном и ложном благе. О свободе воли / Л. Валла; пер. с лат. В. А. Андрушко и др. – Москва: Наука, 1989. – 475 с.

44. Васенин В. А. Информационная безопасность и компьютерный терроризм / В. А. Васенин // Научные и методологические проблемы информационной безопасности. – Москва: МЦНМО, 2004. – С. 67-85. ISBN 5-94057-147-6.

45. Василенко И. А. Геополитика современного мира / И. А. Василенко. – Москва : Гардарики, 2006. – 320 с. ISBN 5-8297-0254-1.

46. Васильев Г. Г. Становление информационной цивилизации и тенденции обновления регулятивной системы общества / Г. Г. Васильева // Роль государства в формировании современного общества. – Москва: Университетский Гуманитарный Лицей, 1998. – С. 50-52.

47. Васильевене Н. Влияние классического философского наследия на развитие прикладной этики (на примере этики организаций) / Н. Васильевене // Философия и этика: сб. науч. трудов. К 70-летию академика А. А. Гусейнова. – Москва: Альфа-М, 2009. – С. 671-672. ISBN: 978-5-98281-172-1.

48. Ващекин Н. П. Безопасность и устойчивое развитие России / Н. П. Ващекин, М. И. Дэлиев, А. Д. Урсул. – Москва : МГУК, 1998. – 446 с. ISBN 5-87827-068-4 : 500 экз.

49. Ващекин Н. П. Цивилизация и Россия на пути к устойчивому развитию: проблемы и перспективы / Н. П. Ващекин, В. А. Лось, А. Д. Урсул. – Москва: МГУК, 1999. – 357 с. ISBN 5-87827-089-7.

50. Вачнадзе Г. Н. Агрессия против разума: информационный империализм / Г. Н. Вачнадзе. – Москава: Политиздат, 1988. – 271 с.

51. Вебер М. Избранные произведения: пер. с нем. / М. Вебер. – Москва: Прогресс, 1990. – 804с. ISBN 5-01-001584-6 (В пер.)

52. Вернадский В. И. Несколько слов о ноосфере / В. И. Вернадский // Ноосферные исследования. – 2013. – Вып. 1(3). – С. 6-17. ISSN 2307-1966.

53. Википедия: Список правил. [Электронный ресурс]. – URL: http://ru.wikipedia.org.

54. Винер Н. Кибернетика, или управление и связь в животном и машине: пер. с англ. И. В. Соловьева / Н. Винер. – Москва: Советское радио, 1958. – 215с.

55. Винер Н. Творец и робот / Н. Винер – Москва: Прогресс, 1996. – 102 с. ISBN 5-17-019210-X : 5000.

56. Виртуальная реальность [Электронный ресурс]. – URL: http://www.gumer.info/bogoslov_Buks/Philos/New_Dict/120.php

57. Возжеников А. В. Основные концептуальные положения национальной безопасности России в XXI веке / А. В. Возжеников, И. Н. Глебов, В. А. Золотарев. – Москва : ЭДАСПАК, 2000. – 48 с. ISBN 5-901248-02-3.

58. Возженников А. В. Государственное управление и национальная безопасность России / А. В. Возженников, А. А. Прохожее. – Москва: РАГС, 2001. – 127с. ISBN 5-7729-0101-X.

59. Волкова И. В. «Информационный империализм» и борьба за духовную деколонизацию Африки (80-е гг.) / И. В. Волкова // Научно-информационный бюллетень. – Москва: Институт Африки АН СССР, 1987. – № 9. – 52 с.

60. Волокитин А. В. Массовая домашняя компьютеризация – необходимый шаг по пути к информационному обществу / А. В. Волокитин // Информационное общество. – Москва, 1999. – Вып. 6. – С. 22-27.

61. Войскунский А. Е. Актуальные психологические проблемы кибер-этики / А. Е. Войскунский, А. И. Нафтульев // Гуманитарная информатика. – Томск: Томск. ун-т, 2007. – Вып. 3. – С. 31-39.

62. Войскунский А. Е. Информационная безопасность: психологические аспекты / А. Е. Войскунский // Национальный психологический журнал. – 2010. - №1(3). – С. 48-53.

63. Войскунский А. Е. Становление киберэтики: исторические основания и современные проблемы /А. Е. Войскунский, О. А. Дорохова // Вопросы философии. – 2010. - № 5, Май. – С. 69-83.

64. Войскунский А. Е. Актуальные проблемы психологии зависимости от Интернета / А. Е. Войскунский // Психологический журнал. – 2004. – Т. 25, № 1. – С. 90-100.

65. Всеобщая декларация прав человека [Электронный ресурс]. – URL: http://www.un.org/ru/documents/decl_conv/declarations.

66. Вудвортс Р. Contemporary schools of psychology, L. 1964. Экспериментальная психология / Р. Вудвортс. – Москва: Издательство иностранной литературы, 1950. – 798 с.

67. Гайкович В. Ю. Основы безопасности информационных технологий / В. Ю. Гайкович, Д. В. Ершов. – Москва: МИФИ, 1995. – 96 с.

68. Галинская И. Л. Этико-правовое пространство информационно-компьютерных технологий / И. Л. Галинская, А. И. Панченко

// Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. – Москва, 2003. – С . 112-132.

69. Галицкий А. В. Защита информации в сети: анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – Москва: ДМК Пресс, 2004. – 616 с. ISBN: 5940742440.

70. Гармонизированные критерии Европейских стран (Information Technology Security Evaluation Criteria, ITSEC) [Электронный ресурс]. – URL: https://www.bsi.bund.de/SharedDocs/ publicationFile.

71. Гарнхэм Э. Искусственный интеллект: Ведение / Э. Гарнхэм // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 75-125.

72. Гельвеций К. А. Мысли и размышления / К. А. Гельвеций. – Сочинения в 2-х томах. – Москва: Мысль,1973. – 1334 с.

73. Гейтс Б. Бизнес со скоростью мысли / Б. Гейтс. – Москва: Русь, 2001. – 456 с. ISBN 5-04-006117-X.

74. Гибсон У. Нейромант / У. Гибсон; пер. с англ. Е. Летова, М. Пчелинцева. – Москва: Аст; Санкт-Петербург: Terra Fantastica, 2000. – 317с. ISBN 5-17-000338-2.

75. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – Москва: РАГС, 1998. – 125 с. ISBN 5-7729-0030-7.

76. Гриняев С. Н. Интеллектуальное противодействие информационному оружию / С. Н. Гриняев. – Москва: Синтег, 1999. – 232 с. ISBN 5-89638-015-1.

77. Гриняев С. Н. Информационное противоборство в современную эпоху / С. Н. Гриняев. [Электронный ресурс]. – URL:http://psyfactor.org.

78. Гриняев С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Минск: Харвест, 2004. – 448 с.

79. Гришина К. В. Вопросы социально-психологического обеспечения деятельности комплексных систем защиты информации / К. В. Гришина, Е. В. Морозова // Безопасность информационных технологий. – 1997. - № 1. – С. 12-17.

80. Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) / Е. В. Громов // Вестник ТГПУ. – 2006. - № 11. – С. 30-35.

81. Гроций Г. О праве войны и мира / Г. Гроций. – Москва: Ладомир, 1994. – 870 с. ISBN 5-86218-149-0.

82. Гоббс Т. Сочинения. В 2 т. Т.2. – Москва: Мысль, 1991. – 736 с. ISBN 5-244-00020-9.

83. Гольбах П.-А. Избранные произведения. В 2 т. / П. А. Гольбах. – Москва: Мысль, 1963. – 1278 с.

84. Гольбах П. Система природы, или о законах мира физического и мира духовного / П. Гольбах. – Москва: ОГИЗ, Соцэкгиз, 1940. – 455 с.

85. Гусейнов А. А. Закон и поступок (Аристотель, И. Кант, М. М. Бахтин) / А. А. Гусейнов // Этическая мысль. – Москва: ИФ РАН, 2001. – Вып. 2 – С. 3-25.

86. Гусейнов А. А. Золотое правило нравственности / А. А. Гусейнов. – Москва: Молодая гвардия, 1988. – 271 с. ISBN 5-235-00244-X.

87. Гусейнов А. А. Размышления о прикладной этике / А. А. Гусейнов // Ведомости Нучно-исследовательского Института прикладной этики. – Тюмень: НИИПЭ, 2004. – Вып. 25. – С. 148-159.

88. Дайзард У. Наступление информационного века / У. Дайзард // Новая технократическая волна на Западе. – Москва: Мысль, 1986. – С. 343-356.

89. Декларация в защиту клонирования и неприкосновенности научных исследований // Человек. – Москва, 1998. – № 3. – С. 20-32.

90. Делокаров К. Х. Глобализация и теория хаоса // Глобализация: синергетический подход / К. Х. Делокаров. – Москва: РАГС, 2002. – 432 с.

91. Дзлиев М. И. Проблемы безопасности: теоретико-методологические аспекты / М. И. Дэлиев, А. Л. Романович, А. Д. Урсул. – Москва: МГУК, 2001. – 192 с. ISBN 5-94746-002-5.

92. Джоуэтт Г. С. Пропаганда и внушение / Г. С. Джоуэтт, В. О'Доннел. – Москва: Мысль, 1988. – 131 с.

93. Доктрина информационной безопасности РФ // Рос. Газ. – 2000. – 28 сент. ISBN 5-86894-938-2.

94. Друкер П. Посткапиталистическое общество / П. Друкер // Новая постиндустриальная волна на Западе. Антология. – Москва: Academia, 1999. – С.70-100.

95. Дробницкий О. Г. Моральная философия: Избранные труды / О. Г. Дробницкий. – Москва: Гардарики, 2002. – 523 с. ISBN 5-8297-0099-9.

96. Дрюккер П. Рынок: как выйти в лидеры, практика и принципы / П. Дрюккер. – Москва: Бук Чамбер Интерн, 1992. – 240 с. ISBN 5-85020-109-2 : Б. ц.

97. Дьякова Е. Г. Информационное неравенство как предмет государственной политики: национальные модели решения проблемы / Е. Г. Дьякова // Общественные трансформации и киберпространство: междисциплинарное исследование: сб. науч. ст. – Санкт-Петербург: Факультет филологии и искусств СПбГУ, 2009. – С. 13-27 с.

98. Евдокимов К. Н. К вопросу о причинах компьютерной преступности в России / К. Н. Евдокимов // Известия ИГЭА. – Иркутск, 2010. – № 6. – С. 167-170.

99. Европейская конвенция о защите прав человека и основных свобод [Электронный ресурс]. – URL: http://www.conventions.ru/view_base.php?id=395.

100. Еременко Д. В. Введение в оценку техники / Д. В. Еременко. – Москва: МНЭПУ, 2002. – 250 с. ISBN 5-7383-0222-2 (в обл.)

101. Ермаков Ю. А. Манипуляция личностью: смысл, приёмы, последствия / Ю. А. Ермаков. – Екатеринбург: Изд-во Урал ун-та, 1999. – 203 с. ISBN 5-7525-0533-X.

102. Емельянов Г. В. Проблемы обеспечения информационно-психологической безопасности России / Г. В. Емельянов, В. Е. Лепский, А. А. Стрельцов // Информационное общество. – Москва, 1999. – Вып. 3. – С. 47-51.

103. Ершов Д. А. Информационная безопасность личности как цель социально-педагогической деятельности / Д. А. Ершов. [Электронный ресурс].– URL:http://scipeople.ru/group/125/topic/196.

104. Заплатинський В. М. Терминология науки о безопасности. Zbornik prispevkov z medzinarodnej vedeckej konferencie «Be-

zhecnostna veda a bezpecnostne vzdelanie» / В. М. Заплатинський. – Liptovsky Mikulas : AOS v Liptovskom Mikulasi, 2006. – 16 с.

105. Захаров М. Ю. Безопасность социума как философско-методологическая проблема / М. Ю. Захаров. – Монино, 1995. – 198 с.

106. Захаров М. Ю. Информационная безопасность социума: социально-философское исследование: автореф. дис. … д-ра филос. наук: 09.00.11 / М. Ю. Захаров. – Ростов-на-Дону, 1998. – 46 с.

107. Зегжда П. Д. Теория и практика обеспечения информационной безопасности / П. Д. Зегжда, Д. П. Зегжда, П. В. Семьянов, С. С. Корт, В. М. Кузьмич, И. Д. Медведовский, А. М. Ивашко, А. П. Баранов. – Москва: Яхтсмен, 1996. – 298 с.

108. Зегжда Д. П. Как построить защищенную информационную систему / Д. П. Зегжда, А. М. Ивашко. – Санкт-Петербург: Мир и семья-95, 1997. – 312 с.

109. Зельцер В. Анонимность выражения мнениях / В. Зельцер. [Электронный ресурс]. – URL:http://wendy.seltzer.org/.

110. Золотов Е. Рождение киборга / Е. Золотов. [Электронный ресурс]. – URL:http://www.computerra.ru/online/ firstpage/politica/169444/t.

111. Известия [Электронный ресурс]. – URL:http://izvestia.ru /tech/2003

112. Иноземцев В. Л. Собственность в постиндустриальном обществе и исторической перспективе / В. Л. Иноземцев // Вопросы философии, 2000. – № 12. – С. 3-13.

113. Информационная безопасность. Актуальные проблемы безопасности социума. – Москва: Оружие и технологии, 2009. – 256 с. ISBN 978-5-93799-043-3.

114. Информационная этика [Электронный ресурс]. – URL: http://webplanet.ru/news/life/2008/09/29/blogs_ftw.html.

115. Информационные вызовы национальной и международной безопасности / И. Ю. Алексеева и др.; под общ. ред. А. В. Федорова, В.Н. Цыгичко. – Москва: ПИР-Центр, 2001. – 328 с. ISBN 5-94013-006-2.

116. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Тер-

мины и определения. ГОСТ 34.003-90. [Электронный ресурс]. – URL: http://db3.nsc.ru:8080/jspui/bitstream/SBRAS/7060/4.

117. Иншаков М. В. Обеспечение информационной безопасности России в условиях становления глобального информационного общества: автореф. дис. … канд. полит. наук / М. В. Иншаков. – Москва, 2007. – 12 с.

118. Йонас Г. Принцип ответственности. Опыт этики для технологической цивилизации / Г. Йонас. – Москва: Айрис-пресс, 2004. – 480 с. ; ISBN 5-8112-0625-9 (в пер.)

119. Кан Г. Грядущий подъем: экономический, политический, социальный / Г. Кан // Новая технократическая волна на Западе. – Москва: Мысль, 1986. – С. 169-206.

120. Кант И. Идея всеобщей истории во всемирно-гражданском плане / И. Кант. – Москва: Наука, 1978. – С. 340-379.

121. Кант И. Сочинения. В 6 т. Т. 4, ч. 1 / И. Кант. – Москва : Мысль, 1965. – 544 с.

122. Кант И. Сочинения. В 8 т. Т. 3 / И. Кант. – Москва: Чоро, 1994. – 584 с.

123. Капуро Р. Информационная этика / Р. Капуро // Информационное общество. – 2010. – Вып. 5. – С. 5-15.

124. Карамнов А. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах / А. Ю. Карамнов, М. Ю. Дворецкий // Вестник ВИ МВД России. – 2011. – № 2. – С. 166-169.

125. Касенова М. Б. Интернет и международное публичное право: ретроспектива доктринальных подходов / М. Б. Касенова. [Электронный ресурс]. – URL: http://lexandbusiness.ru/view-article.php?id=577.

126. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – Москва: ГУ ВШЭ, 2000. – 608 с. ISBN 5-7598-0069-8.

127. Киттлер Ф. А. Мир символического – мир машины / Ф. А. Киттлер // Философско-литературный журнал ЛОГОС. – Москва, 2010. – № 1(74). – С. 5-22.

128. Коваль Е. В. Этика современного общества, как современный этап развития этики / Е. В. Коваль // Вестн. Чуваш. ун-та. – 2009. - № 4. – С. 133-139.

129. Колин К. К. Информационная цивилизация / К. К. Колин. – Москва: Ин-т проблем информатики РАН, 2001. – 112 с. ISBN 5-88018-290-8.

130. Коновалова Л. В. Прикладная этика / Коновалова Л. В. – Москва : ИФРАН, 1998. – 217 с.

131. Кононов О. А. Социальные и этические аспекты обеспечения информационной безопасности. Проблемы управления / О. А. Кононов, О. В. Кононова. – Москва: Сенсидат-Плюс, 2009. – Вып. 1. – С. 76-79.

132. Константин Л. Человеческий фактор в программировании / Л. Константин. – Москва: Символ-Плюс, 2004. – 185 с. ISBN 5-93286-044-8 : 2000.

133. Концепция информационной безопасности Российской Федерации // Информационное общество. – 1995. – Вып. 6. – С. 53-78.

134. Копылов В. А. Информационное право / В. А. Копылов. – Москва: Юристъ, 2002. – 512 с. ISBN 5-7975-0472-3.

135. Корсунцев И. Г. Субъект в технологическую эпоху / И. Г. Корсунцев. – Москва: Российское филос. общество, 1999. – 219 с. ISBN 5-8081-0023-2.

136. Кочергин А. Н. Философия и глобальные проблемы / А. Н. Кочергин. – Москва: РОУ, 1996. – 176 с. ISBN 5-204-00067-4 : Б. ц.

137. Критерии безопасности информационных технологий. [Электронный ресурс]. – URL: http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf.

138. Критерии оценки доверенных компьютерных систем – стандарт Министерства обороны США (англ. Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, DoD 5200.28-STD, December 26, 1985) [Электронный ресурс]. – URL: http://mind-control.

139. Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика / В. Л. Кудрявцев // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки применения его положений с учетом задач дальнейшего

укрепления экономического правопорядка. – Нижний Новгород, 2012. – С. 69-76.

140. Кудрявцев В. Н. Наука клеймит псевдонауку / В. Н. Кудрявцев, Б. Н. Топорнин // Известия. – 1998. - № 130. – 17 июля.

141. Кузнецов В. Н. Российская идеология XXI века в обеспечении эффективности и безопасности динамично-устойчивого развития России / В. Н. Кузнецов. – [Электронный ресурс]. – URL: http://spkurdyumov.narod.ru/Kuznetsov25.htm.

142. Лаврухин А. Н. Роль принципа структурно-политического плюрализма в становлении информационного общества / А. Н. Лаврухин // Техника, общество и окружающая среда: материалы междунар. науч. конф. – Москва: Ин-т филос. РАН, 1998. – 150 с. ISBN 5-94101-090-7 (в обл.)

143. Лазар М. Г. Этика науки: Философские аспекты соотношения науки и морали / М. Г. Лазар. – Ленинград: Ленинград. ун-т, 1985. – 126 с.

144. Лазарев И. А. Информационная безопасность / И. А. Лазарева. – Москва : МГЦНТИ, 1997. – 336 с.

145. Лайнбарджер П. Психологическая война / П. Лайнбарджер. – Москва: Воениздат, 1962. – 351 с.

146. Левин В. К. Защита информации в информационно-вычислительных системах и сетях / В. К. Левин // Програмирование. – 2004. – № 5. – С. 5-16.

147. Лейбниц Г.-В. Сочинения. В 4 т. Т. I / Г.-В. Лейбниц. – Москва: Мысль, 1982. – 556 с.

148. Лешкевич Т. Г. Философия науки: Традиции и новации / Т. Г. Лешкевич. – Москва: ПРИОР, 2001. – 428 с. ISBN 5-7990-0477-9.

149. Лири Э. Аминокислоты: будущее компьютирования в 1990-х годах / Э. Лири // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 49-58.

150. Локк Дж. Сочинения. В 3 т. Т. 3 / Дж. Локк. – Москва: Мысль, 1985. – 634 с.

151. Лопатин В. Н. Безопасность - информационный выбор России в XXI в. / В. Н. Лопатин. – Москва: Космосинформ, 2003. – 194 с. ISBN 5-93598-030-4.

152. Лопатин В. Н. Информационная безопасность России: Человек, общество, государств / Лопатин В. Н. // Безопасность человека и общества. – Москва: Фонд «Университет», 2000. – 428 с. ISBN 5-93598-030-4.

153. Лопатин В. Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации (проект) / В. Н. Лопатин. – Москва: Космосинформ, 1998. – 159 с.

154. Любутин К. Н. Фейербах: философская антропология / К. Н. Любутин. – Свердловск: Урал. ун-т, 1988. – 127 с.

155. Макаренко С. И. Информационная безопасность / С. И. Макаренко. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

156. Макгован У. Телекоммуникации и мировая конкуренция / У. Макгован // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 38-42.

157. Макеев А. В. Основы политики национальной безопасности: структурогенез и механизм реализации: автореф. дис. ... д-ра полит. наук: 23.00.02/ А. В. Макеев. – Москва: МГУ, 1999. – 42 с.

158. Малинецкий Г. Г. Новое в синергетике. Новая реальность, новые проблемы, новое поколение / Г. Г. Малинецкий. – Москва: Наука, 2007. – 384 с. ISBN 5-02-033958-X (В пер.)

159. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – Москва: Горячая линия-Телеком, 2001. – 148 с. ISBN 5-93517-062-0.

160. Малюк А. А. Гуманитарные аспекты информационной безопасности, образование, система подготовки специалистов в области информационной безопасности / А. А. Малюк, О. Ю. Полянская // Вестник РГНФ . – 2011. – № 4(65). – С. 72-78.

161. Малюк А. А. Кодекс этики в сфере информационных технологий как основа обеспечения информационной безопасности / А. А. Малюк, О. Ю. Полянская. [Электронный ресурс]. – URL: http://library.mephi.ru/data/scientific-sessions/2007/z14/2-1-23.doc.

162. Манжуева О. М. Три уровня компьютерной этики Т. Бинема / О. М. Манжуева. – Перспективы науки. – 2014. – № 2(53). – С. 117-120.

163. Манойло А. В. Государственная информационная политика в особых условиях. / А. В. Манойло. – Москва: МИФИ, 2003. – 388 с. ISBN 5-7262-0510-3.

164. Манойло А. В. Информационно-психологическая безопасность / А. В. Манойло, А. И. Петренко, Д. Б. Фролов // Безопасность информационных технологий. – 2004. – №1. – С. 17-21.

165. Манойло А. В. Информационно-психологическая безопасность современного информационного общества. / А. В. Манойло, А. И. Петренко // Стратегическая стабильность. – 2003. – №3. – С. 59-64.

166. Манойло А. В. Технологии несилового разрешения современных конфликтов. / А.В. Манойло. – Москва: Горячая линия – Телеком, 2008. – 392 с. ISBN: 978-5-9912-0414-9.

167. Мантатов В. В. Стратегия разума: экологическая этика и устойчивое развитие: в 2-х т. / В. В. Мантатов. – Улан-Удэ: Бурятское книжное издательство, 1998. – Т. 1. – 204 с. ISBN 5-7411-0411-8.

168. Мантатов В. В. Стратегия разума: экологическая этика и устойчивое развитие: в 2-х т. / В. В. Мантатов. – Улан-Удэ: Бурятское книжное издательство, 2000. – Т. 2. – 219 с. ISBN 5-7411-0411-8.

169. Мантатов В. В. Теория устойчивого развития: онтология и методология / В. В. Мантатов. – Улан-Удэ: ВСГУТУ, 2009. – 148 с. ISBN 978-5-89230-338-5.

170. Мантатов В. В. Этика устойчивого развития в информационную эпоху / В. В Мантатов, Л. В. Мантатова. – Улан-Удэ: Бурятское книжное издательство, 2002. – 185 с. ISBN 5-7411-0414-2 : 500.

171. Мантатова Л. В. Стратегия развития: Ценности новой цивилизации / Л. В. Мантатова. – Улан-Удэ: ВСГТУ, 2004. – 242 с.

172. Мантатова Л. В. Философская антропология: основные понятия / Л. В. Мантатова. – Улан-Удэ: ВСГУТУ, 2001. – 18 с. ISBN: 5741104134.

173. Маркс К. Соч. Т.6 / К. Маркс, Ф. Энгельс. – Москва: Государственное издательство политической литературы, 1955. – 616 с.

174. Мастерман Л. Обучение языку средств массовой информации / Л. Мастерман // Специалист. – 1993. – № 4. – С. 22-23.

175. Мележик И. Н. Понятие, происхождение и природа государства в политическом учении Т. Гоббса / И. Н. Мележик // Актуальные проблемы истории политических и правовых учений. – Москва, 1990. – С. 104-122.

176. Мельник И. К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / И. К. Мельник, Г. В. Грачев. – Москва: Эксмо, 2002. – 112 с. ISBN 5-201-02023-2.

177. Мелюхин И. С. Информационное общество и баланс интересов государства и личности / И. С. Мелюхин // Информационное общество. – Москва, 1997. – С. 4-6.

178. Мелюхин И. С. Информационное общество: истоки, проблемы, тенденции развития / И. С. Мелюхин. – Москва: Издательство МГУ, 1999. – 208 с. ISBN 5-211-04096-1.

179. Мелюхин И. С. Концепции информационного общества и роль государства / И. С. Мелюхин // Информационные ресурсы России. – 1997. – № 2. – С. 33-35.

180. Мескон М. Х. Основы менеджмента / М. Х. Мескон, М. Альберт, Ф. Хедоури. – Москва: Дело, 1993. – 704 с. ISBN 5-7749-0047-9 : 10 000 экз.

181. Метлер-Мейбом Б. Социальные цены в информационном обществе: размышление о коммуникативной экологии. Информационная революция: наука, экономика, технология / Б. Метлер-Мейбом. – Москва: ИНИОН РАН, 1993. – С. 161-174.

182. Миллер Г. У. Качественная программа: будущее информационной технологии / Г. У. Миллер. – Москва: ИНИОН РАН, 1993. – С. 63-75.

183. Милль Д. С. Утилитарианизм / Д. С. Милль. – СПб.: И. П. Перевозин, 1900. – 427 с.

184. Минзов А. С. Профессиональная этика специалиста в области безопасности бизнеса / А. С. Минзов. – Москва: МЭИ, 2005. – 92 с. ISBN 5-7046-1329-2.

185. Многомерный образ человека: Комплексное междисциплинарное исследование человека. – Москва: Наука, 2001. – 239 с. ISBN 5-02-008361-5.

186. Модельный Уголовный кодекс стран СНГ [Электронный ресурс]. – URL: http://online.zakon.kz.

187. Модельный закон об информатизации, информации и защите информации. Принят на двадцать шестом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (Постановление от 18 ноября 2005 года № 26-7) [Электронный ресурс]. – URL: http://base.spinform.ru/show_doc.fwx?rgn=63035.

188. Моисеев Н. Н. Судьба цивилизации. Путь разума / Н. Н. Моисеев. – Москва: МГВП КОКС, 1998. – 228 с. ISBN 5-7859-0118-8.

189. Моисеев Н. Н. Информационное общество как этап новейшей истории / Н. Н. Моисеев // Свободная мысль. – 1996. – № 1. – С. 81-83.

190. Моррис-Сузуки Т. По ту сторону компутоутопии: Информация, автоматизация и демократия Японии / Т. Моррис-Сузуки // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 128-161.

191. Мусхелишвили Н. Л. Ценностная рефлексия и конфликты в разделенном обществе / Н. Л. Мусхелишвили, В. М. Сергеев, Ю. А. Шрейдер // Вопросы философии. – 1996. – № 11. – С. 18-36.

192. Мыслители Греции. От мифа к логике: сочинения / сост. В. В. Шкода. – Москва: Эксмо-Пресс; Харьков: Фолио, 1998. – 832 с. ISBN 5-04-001264-0 (ЭКСМО-Пресс).

193. Назаретян А. П. Агрессия, мораль и кризисы в развитии мировой культуры / А. П. Назаретян. – Москва: Наследие, 1996. – 183 с. ISBN 5-86562-013-4 : Б. ц.

194. Назаров В. Н. Прикладная этика / В. Н. Назаров. – Москва: Гардарики, 2005. – 302 с. ISBN 5-8297-0242-8 (в пер.)

195. Наумов В. Б. Право и Интернет: очерки теории и практики / В. Б. Наумов. – Москва: Книжный дом «Университет», 2002. – 432 с. ISBN 5-8013-0155-0.

196. Национальный план защиты инфраструктуры США. National Infrastructure Protection Plan – NIPP [Электронный ресурс]. – URL: http://net.educause.edu.

197. Некрасов С. И. Философия науки и техники: тематический словарь справочник / С. И. Некрасов, Н. А. Некрасова. – Орёл: ОГУ, 2010. – 289 с. ISBN 978-5-7876-0146-6.

198. Николо Макиавелли. Государь. / Н. Макиавелли. – Москва : Олма Медиа Групп, 2011. – 512 с. ISBN 978-5-373-04147-8 (в пер.)

199. Нисневич Ю. А. Информация и власть / Ю. А. Нисневич. – Москва: Мысль, 2000. – 175 с. ISBN 5-244-00973-7.

200. Новая философская энциклопедия. В 4 т. Т. 1. – Москва: Мысль, 2010. – 721 с. ISBN 5-244-00961-3.

201. Новейший философский словарь / Сост. А. А. Грицанов. – Минск: Изд. В. М. Скакун, 1998. – 896 с. ISBN 985-6235-17-0.

202. Общая теория национальной безопасности / под общ. ред. А. А. Прохожева. – Москва: РАГС, 2002. – 320 с. ISBN 5-7729-0138-9.

203. Общие критерии оценки безопасности информационных технологий» международный стандарт. (Common Criteria for Information Technology Security Evaluation Security) [Электронный ресурс]. – URL: http://www.ipa.go.jp/security/jisec/cc/documents.

204. Огородов Д. В. Правовые отношения в информационной сфере: автореф. дис. …канд. юрид. наук / Д. В. Огородов. – Москва, 2002. – 25 с.

205. Официальный сайт МВД России [Электронный ресурс]. – URL: http://mvd.ru.

206. Павлович О. В. Антропологическая парадигма национальной безопасности в философской системе Томаса Гоббса / О. В. Павлович // Вестник ОГУ. – 2011. - №7 (126). – С. 62-67.

207. Панарин А. С. Стратегическая нестабильность в XXI веке / А. С. Панарин. – Москва: Алгоритм, 2003. – 560 с. ISBN 5-9265-0111-3 (в пер.)

208. Перчук Е. Е. Информатизация и информационная безопасность: автореф. дис. … канд. филос. наук / Е. Е. Перчук. – Москва: [б. и.], 2002. – 31 с.

209. Петров В. П. Информационная безопасность России в условиях глобализации / В. П. Петров // Политическое образование. – 2014. ISBN 978-5-93196-814-8. – [Электронный ресурс]. – URL: http://www.lawinrussia.ru.

210. Петрунин Ю. Ю. Этика бизнеса Петрунин / Ю. Ю. Петрунин, В. К. Борисов. – Москва: Дело, 2000. – 280 с. ISBN 5-7749-0199-8.

211. Поздняков А. И. Информационная безопасность / А. И. Поздняков // Безопасность. – 1992. – № 6. – С. 14-23.

212. Поздняков А. И. Информационная безопасность личности, общества и государства / А. И. Поздняков // Военная мысль. – 1993. – № 10. – С. 13-14.

213. Поздняков А.И. Информационная безопасность страны и Вооруженных Сил // Национальная безопасность: актуальные проблемы. – Москва: ВАГШ, 1999. – С.171-173.

214. Поликарпов А. В. Социально-философские аспекты информационной безопасности России: автореф. дис. … канд. филос. наук / А. В. Поликарпов. – Ростов-на-Дону: [б. и.], 2000. – 18 с.

215. Прохожев А. А. Национальная безопасность основы теории, сущность проблемы / А. А. Прохожев. – Москва: РАГС, 1996. – 27 с.

216. Попов В. Д. Парадигмы исследования информационных процессов / В. Д. Попов. – Москва: РАГС, 2010. – 60 с.

217. Почему обществу и Церкви нужен, безопасный Интернет [Электронный ресурс]. – URL: http://borisov-spas.by/pravoslavny-e-stat-i.

218. Почепцов Г. Г. Информационная политика и безопасность современных государств / Г. Г. Почепцев. [Электронный ресурс]. – URL: http://psyfactor.org/.

219. Почепцов Г. Г. Информационные войны / Г. Г. Почепцев. – Москва: Рефл-бук, 2000. – 280 с. ISBN 5-87983-087-х (Рефл-бук).

220. Почепцов Г. Г. Информационно-психологическая война / Г. Г. Почепцев. – Москва: СИНТЕГ, 2000. – 180 с. ISBN 5-89638-028-3.

221. Пошью Л. Дж. О компьютерном этическом кодексе для российских институтов и университетов / Л. Дж. Пошью // Науч. и техн. б-ки. – 1998. – №7. - С. 12-20

222. Правила сетевого этикета // Библиотечная этика в странах мира / Сост. В. Р. Фирсов, И. А. Трушина. – Санкт-Петербург: РНБ, 2010. – 156 с. ISBN 5-8192-0122-1.

223. Пригожин И. Порядок из хаоса: Новый диалог человека с природой / И. Пригожин, И. Стенгерс. – Москва: Прогресс,1986. – 432 с.

224. Пригожин И. Р. Сетевое общество / И. Р. Пригожин // Социологические исследования. – 2008. – № 1. – С. 24-27.

225. Прихожан А. М. Информационная безопасность и развитие информационной культуры личности / А. М. Прихожан // Мир психологии. – 2010. – № 3. – С. 135-141.

226. Программа действий. Повестка дня на XXI век и другие документы конференций в Рио-де-Жанейро. – Женева, 1994. – С. 1.

227. Программа ЮНЕСКО «Информация для всех» [Электронный ресурс]. – URL: http://old.zntu.edu.ua.

228. Программы фильтры для ограничения информации для граждан через Интернет, устанавливаемые государством [Электронный ресурс]. – URL: http://www/opennetinitiative.org.

229. Пурник А. В. От Библиотеки к Библиотеке 2.0 / А. В. Пурник // Социолог и психолог в библиотеке: Сб. статей и материалов. Вып. VII / Рос.гос. б-ка для молодёжи; Рос. гос. дет. б-ка; ред. - сост. М. М. Самохина. – Москва, 2010. – С. 6-10.

230. Рабочий документ для подготовительной группы по правам человека, силе закона и информационному обществу, п. 8, 15 сентября 2004 г. (об осуждении цензуры в действиях поисковых машин во Франции, Германии и Китае) [Электронный ресурс]. – URL: http://cyber.law.harvard.edu/filtering/google/results1html.

231. Райбекас А. Я. Вещь, свойство, отношение как философские категории / А. Я. Райбекас. – Томск: Томск. ун-т, 1977. – 244 с.

232. Ракитов А. И. Информационная революция как фактор экономического и социального развития / А. И. Ракитов // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1993. – С. 5-17.

233. Ракитов А. И. Новый подход к взаимосвязи истории, информации и культуры: пример России / А. И. Ракитов // Вопросы философии. – Москва, 1994. – С. 45- 61.

234. Ракитов А. И. Новый подход к взаимосвязи истории, информации и культуры: пример России / А. И. Ракитов // Вопросы философии. – 1994. – № 4. – С. 56-68.

235. Ракчеева Н. Е. Государство. Платон / Н. Е. Ракчеева. – Москва: МАКС Пресс, 2001. – 202 с. ISBN 5-317-00257-5.

236. Рассолов И. М. Право и Интернет / И. М. Рассолов. – Москва: Норма, 2003. – 210 с. ISBN 5-89123-711-3 (в обл.)

237. Расторгуев С. П. Информационная война / С. П. Расторгуев. – Москва: Радио и связь, 1998. – 416 с. ISBN 5-256-01399-8.

238. Расторгуев С. П. Философия информационной войны / С. П. Расторгуев. – Москва: Вузовская книга, 2001. – 468 с. ISBN 5-89502-346-0.

239. Расторгуев С. П. Информационная война. Проблемы и модели. Экзистенциальная математика. / С. П. Расторгуев. – Москва: Гелиос АРВ, 2006. – 240 с. ISBN 5-85438-145-1.

240. Редикульцев С. Google и "Яндекс" заглядывают в личную информацию пользователей / С. Редикульцев. [Электронный ресурс]. – URL: http://www.vesti.ru/news.

241. Робертсон Д. С. Информационная революция / Д. С. Робертсон // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 17-27.

242. Рузавин Г. И. Методология научного исследования / Г. И. Рузавин. – Москва: ЮНИТИ-ДАНА, 1999. – 288 с. ISBN 5-238-00085-5.

243. Руководящие документы Гостехкомиссии России [Электронный ресурс]. – URL: http://www.ivtechno.ru/files/rd_filter.pdf.

244. Садовский В. Н. Основания общей теории систем / В. Н. Садовский. – Москва: Наука, 1974. – 280 с.

245. Сандакова Л. Г. Информационно-технологическая парадигма образования: гуманистическая сущность и концептуальные основы: автореф. дис. … д-ра филос. наук: 09.00.11. – Улан-Удэ, 2003. – 40 с.

246. Сандакова Л. Г. Философия образования: гуманитарная информационно-технологическая модель / Л. Г. Сандакова. – Москва: Компания Спутник+, 2002. – 153 с. ISBN 5-93406-453-3 (в обл.)

247. Селезнев И. А. Война и идеологическая борьба / И. А. Селезнев. – Москва: Воениздат, 1974. – 156 с.

248. Семененко В. А. Информационная безопасность / В. А. Семененко. – Москва: МГИУ, 2005. – 215 с. ISBN 978-5-2760-1876-8.

249. Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации [Электронный ресурс]. – URL: http://www.docload.ru/Basesdoc/6/6316/index.htm.

250. Ситкевич Н. В. Рассмотрение в информационной этике дилеммного характера правовых проблем современного общества. Исторические, философские, политические и юридические науки, культурология и искусствоведение / Н. В. Ситкевич // Вопросы теории и практики. – Тамбов: Грамота, 2014. – № 3 (41): в 2-х ч. – Ч. I. – С. 147-150.

251. Скворцов А. А. Мораль и современные информационные технологии / А. А. Скворцов. [Электронный ресурс]. – URL: http://iph.ras.ru/uplfile/ethics/RC/prog/applied/IP.html.

252. Словарь гендерных терминов [Электронный ресурс]. – URL: http://www.owl.ru/gender/096.htm.

253. Смолян Г. Л. Сетевые информационные технологии и проблемы безопасности личности / Г. Л. Смолян // Информационное общество. – Москва,1999. – № 1. – С. 3-8.

254. Смолян Г. Л. Человек и компьютер: социально-философские аспекты автоматизации управления и обработки информации / Г. Л. Смолян. – Москва: Политиздат, 1981. – 192с.

255. Соколов А. В. На пути к Кодексу библиотечной этики. Новая редакция нуждается в доработке / А. В. Соколов // Библиотечное дело. – 2011. – № 06 (144)11. – С. 33-35.

256. Солопов П. Е. Философские проблемы виртуалистики: автореф. дис. ... канд. филос. наук: 09.00.08 / П. Е. Солопов. – Москва: Моск. гос. ун-т сервиса, 2000. – 22 с.

257. Спенсер Г. Социальная статика / Г. Спенсер. – Киев: Гама-Принт, 2013. – 496 с. ISBN 978-966-1645-90-4.

258. Старовойтов А. В. Информационное обеспечение государственного управления / В. А. Никитов, Е. И. Орлов, А. В. Старовойтов, Г. И. Савин. – Москва: Славянский диалог, 2000. – 415 с. ISBN 5-85468-010-6.

259. Стоинер Т. К новой теории информации / Т. Стоинер // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1992. – С. 42-49.

260. Стоиньер Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоинер // Новая технократическая волна на Западе. – Москва: Мысль, 1986. – С. 393- 421.

261. Стрельцов А. А. Содержание понятия «обеспечение информационной безопасности» / А. А. Стрельцов // Информационное общество. – 2001. – № 4. – С. 10-16.

262. Струнин В. И. Академическая мобильность как приоритетное направление развития современного профессионального образования / В. И. Струнин, С. Л. Тимкин, Т. Ю. Стукен [Электронный ресурс]. – URL: http://ou.tsu.ru/seminars/eois2012.

263. Стюгин М. А. Защита систем от исследования. Методы и модели построения защищенных систем и управления информацией в конфликте / М. А. Стюгин. – Москва: РРГУ, 2011. – 132 с.

264. Субетто А. И. Сочинения. Ноосферизм: В 13 томах. Т. 7 Системология образования и образованиеведение / А. И. Субетто. – Кострома: КГУ им. Н.А. Некрасова, 2007. – 520 с. ISBN 5-7591-0737-2.

265. США. Конституция и права граждан / Под ред. В. А. Власихина. – Москва: Мысль, 1987. – 315 с.

266. Сычев М. П. Киберпреступность и подготовка специалистов по борьбе с ней в России / Н. В. Медведев, М. П. Сычев, И. Б. Федоров // Информационные технологии. – Москва, 2005. – №9. – С. 2-7.

267. Судебное заседание по делу диссидентов на основе информации представленной Yahoo! [Электронный ресурс]. – URL: http://www/rsf.org/article.php3?id_article=16402.

268. Теория социальной ответственности [Электронный ресурс]. – URL: http://buklib.net/books/27296.

269. Титаренко А. И. Антиидеи. Опыт социально-этического анализа. Издание второе, дополненное / А. И. Титаренко. – Москва: Политиздат, 1984. – 480 с.

270. Тонконогов А. В. Информационно-психологическая безопасность в системе духовной безопасности современной России / А. В. Тонконогов // Власть. – 2010. – № 6. – С. 53-56.

271. Тоффлер Э. Метаморфозы власти / Э. Тоффлер. – Москва: АСТ, 2003. – 669 с. ISBN 5-17-004183-7 : 3000.

272. Тоффлер Э. Третья волна / Э. Тоффлер. – Москва: АСТ, 1999. – 794с. ISBN 978-5-17-062498-0 (АСТ)

273. Трахтенберг А. Д. Интернет как пространство утопии в современном постмодернизме / А. Д. Трахтенберг // Общественные трансформации и киберпространство: междисциплинарные исследования. – Санкт-Петербург, 2009. – С. 170-185.

274. Триняк В. Ю. Информационная безопасность как социально-культурный феномен (Социально-философское исследование): автореф. дис. … канд. филос. наук: 09.00.03 / В. Ю. Триняк. – Днепропетровск [б. и.], 2009. – 29 с.

275. Турен А. Возвращение человека действующего. Очерк социологии / А. Турен. – Москва: Научный мир, 1998. – 204 с. ISBN 5-89176-042-8.

276. Уголовный кодекс Российской Федерации. – Москва : Проспект, КноРус, 2010. – 176 с. ISBN 978-5-406-01018-1 : Б. ц.

277. Уголовный кодекс Франции. – Санкт-Петербург: Изд-во «Юридический центр Пресс», 2002. – 650 стр.

278. Уголовный кодекс ФРГ. – Москва : Юрид. колледж МГУ, 1996. – 202 с.

279. Уголовный кодекс Федеративной Республики Германии. Особенная часть. [Электронный ресурс]. – URL: http://law.edu.ru/norm/norm.asp?normID=1242733&subID=100102942,100102944#text.

280. У-Цзы. Сунь-Цзы. Искусство войны / У-Цзы. Пер. Н. И. Конрад.– Москва: Эксмо, 2011. – 476 с. ISBN 978-5-699-52799-1 (в пер.)

281. Управление государственными информационными системами: элементы стратегии и политики // Информационная революция: наука, экономика, технология. – Москва: ИНИОН РАН, 1999. – С. 202-235.

282. Урсул А. Д. Природа информации (Философский очерк) / А. Д. Урсул. – Москва: Политиздат, 1968. – 288 с.

283. Урсул А. Д., Цырдя Т. (Ф). Н. Информационная безопасность. Сущность, содержание и принципы ее обеспечения / А. Д. Урсул, Т. (Ф). Н. Цырдя [Электронный ресурс]. – URL: http://security.ase.md/publ/ru/pubru22.html.

284. Уэбстер Ф. Теории информационного общества // Ф. Уэбстер. – Москва: Аспект Пресс, 2004. – 400 с. ISBN 5-7567-0342-х : 5000.

285. Фалько В. И. Философия виртуальности: Подходы и принципы, проблемы и перспективы / В. И. Фалько. – Москва: МАИ, 2000. – 92 с.

286. Фатьянов А. А. Информация как объект права / А. А. Фатьянов // Информационная безопасность России в условиях глобального информационного общества. – Москва, 2001. – С. 47-52.

287. Федоров И. Ф. Философия общего дела / И. Ф. Федоров. – Москва: Книга по требованию, 2012. – 755 с. ISBN: 978-5-699-28019-3.

288. Федотов А. В. Базовые теории медиаобразования / А. В. Федотов // Общественные трансформации и киберпространство: междисциплинарные исследования. – Санкт-Петербург : Факультет филологии и искусств, 2009. –С. 103-132.

289. Федотов Н. Германия ужесточает закон о защите информации. Info watch / Н. Федотов. [Электронный ресурс]. – URL: http://www/comprice.ru/articles/detali.php.

290. Филина О. А. Проблемы современной информационной этики: автореф. дис. … канд. филос. наук: 09.00.05 / О. А. Филина. – Тула: [б. и.], 2009. – 19 с.

291. Филина О. А. Социальные, культурно-исторические и ценностные основания информационной этики / О. А. Филина // Научные Ведомости Белгородского Государственного Университета. – 2009. – № 9(10). – С. 228-233.

292. Философский энциклопедический словарь. – Москва: Инфра-М, 1998. – 576 с. ISBN 5-86225-403-Х (В пер.) : Б. ц.

293. Флягина И. А. Реклама как специфический вид массовой коммуникации и социокультурная динамика / И. А. Флягина // Мир психологии. – Москва. – 2000. – С.67-83.

294. Французская Республика: Конституция и законодательные акты / Сост. и пер. с фр. В. В. Маклаков и др. – Москва: Прогресс,1989. – 448 с.

295. Фролов Д. Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом / Д.

Б. Фролов, Е. В. Старостина // Законодательство и экономика. – 2005. – № 5. – С. 26-30.

296. Фролов И. Т. Избранные труды. Т.2: Философия и история генетики / И. Т. Фролов. – Москва: Республика, 2002. – 540 с. ISBN 5-250-01868-8.

297. Фромм Э. Гуманистический психоанализ / Э. Фромм. – Санкт-Петербург : Питер, 2002. – 544 с. ISBN 5-94723-079-8.

298. Хлебников Г. В. Философия информации Лучано Флориди [Электронный ресурс] / Г. В. Хлебникова. – Режим доступа : http://www.inion.ru/ (дата обращения: 11.03.2014).

299. Хофман Л. Дж. Современные методы защиты информации: Пер. с англ. / Л. Дж. Хофман. – Москва: Сов. Радио, 1980. – 264 с.

300. Циолковский К. Э. Промышленное освоение космоса / К. Э. Циолковский. – Москва: Машиностроение, 1989. – 278 с.

301. Ципелла Т. Рассматривая «великое информационное общество» в перспективе / Т. Ципелла // Информационная революция: наука, экономика, технология. – Москва, 1992. – С. 125-128.

302. Цыганков В. Д. Психотроника и безопасность России / В. Д. Цыганков. – Москва: Синтег, 2003. – 136 с. ISBN 5-89638-066-6 (в обл.)

303. Цырендоржиева Д. Ш. Системный метод исследования общества / Д. Ш. Цырендоржиева. – Москва: Спутник+, 2002. – 125 с. ISBN 5-93406-246-8

304. Цырендоржиева Д. Ш. Системный подход: сущность и возникновение. / Д. Ш. Цырендоржиева. – Москва: Спутник+, 2002. – 122 с. ISBN 5-3406-201-8.

305. Черепанова М. В. Актуализация этических кодексов в контексте современной культуры / М. В. Черепанова // Известия Томского политехнического университета. – 2013. – Т. 322. – № 6. – С. 92-95.

306. Черешкин Д. С. Нелегкая судьба российской информатизации / Д. С. Черешкин, Г. Л. Смолян // Информационное общество. – 2008. – Вып. 1-2. – С. 47-71.

307. Черешкин Д. С. Сетевая информационная революция / Д. С. Черешкин, Г. Л. Смолян // Информационные ресурсы России. – 1997. – № 4. – С. 15-18.

308. Чернов А. А. Становление глобального информационного общества: проблемы и перспективы / А. А. Чернов. – Москва: Дашков и К°, 2003. – 232 с. ISBN 5-94798-251-X : 1000.

309. Чижевский А. Л. Космический пульс жизни: Земля в объятиях Солнца. Гелиотараксия / А. Л. Чижевский. – Москва: Мысль, 1995. – 768 с.

310. Чижик П. И. Духовная безопасность российского общества как фактор военной безопасности государства: автореф. дис. ... д-ра филос. наук: 23.00.02 / П. И. Чижик. – Москва: Военный университет, 2000. – 46 с.

311. Шамраев А. В. Правовое регулирование информационных технологий. Анализ проблем и основные документы. Версия 1.0. / А. В. Шамраев. – Москва: Статус, 2003. – 113 с. ISBN 5-8354-0127-2 : 2500.

312. Шамсуев М.-Э. Х. Теоретические аспекты изучения информационной безопасности / М.-Э. Х. Шамсуев // Теория и практика общественного развития. – 2010. – № 2. – С. 319-325.

313. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – Москва: ИЛ, 1963. – С. 333-369.

314. Шерстюк В. П. МГУ: научные исследования в области информационной безопасности / В. П. Шерстюк // Информационное общество. – 2005. – Вып. 1. – С. 48-53.

315. Шерстюк В. П. О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности / В. П. Шерстюк // Научные и методологические проблемы информационной безопасности. – Москва: МЦНМО, 2004. – С. 37-47.

316. Шершнев Л. И. (под. ред.) Безопасность человека / Коллектив авторов. – Москва: Фонд национальной и международной безопасности, 1994. – 470 с. ISBN 5-94013-006-2.

317. Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации / Ю. В. Гаврилин, А. В. Пушкин, Е. А. Соцков, Н. Г. Шурухнов. – Москва: Щит-М, 1999. – 254 с. ISBN 5-8041-0117-X.

318. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – Москва: Книжный мир, 2009. – 352 с. ISBN 978-5-8041-0357-7.

319. Эйген М. Игра жизни / М. Эйген, Р. Винклер. – Москва: Наука, 1979. – 123 с.

320. Эмм Д. Киберпреступность и закон: обзор положений законодательства Великобритании, касающихся компьютерной преступности / Д. Эмм. [Электронный ресурс]. – URL: http://www/comprice.ru/articles.

321. Эллюль Ж. Другая революция // Новая технократическая волна на Западе. – Москва: Прогресс, 1986. – С. 147-153.

322. Этика и права человека в информационном обществе: материалы Европейской региональной конференции. – Москва: Межрегиональный центр библиотечного сотрудничества, 2009. – 60 с. ISBN 978-5-91515-025-5 : 1000.

323. Этические аспекты новых технологий. Обзор. – Москва: Права человека, 2007. – 102 с. ISBN 978-5-7712-0379-9.

324. Этический кодекс для информационного общества (проект). [Электронный ресурс]. – URL: http://www.osu.ru/docs/kodeks_ethics_info.doc.

325. Эшби У. Введение в кибернетику / У. Эшби. – Москва: Иностр. лит-ра, 1959. – 432 с.

326. Юнг К. Г. Проблемы души нашего времени / К. Г. Юнг. – Москва: Прогресс-Универс, 1993. – 329 с.

327. Юсупов Р. М. Научно-методологические основы информатизации / Р. М. Юсупов, В. П. Заболотский. – Санкт-Петербург: Наука, 2000. – 455 с. ISBN 5-02-024929-7.

328. Ядрышников Е. В. Основные положения проекта Этического кодекса сети Интернет / Е. В. Ядрышников. – [Электронный ресурс]. – URL: http: // www. inethics.com/ru/.

329. Яновский Р. Г. Глобальные изменения и социальная безопасность / Р. Г. Яновский. – Москва : Academia, 1999. – 358 с. ISBN 5-87444-087-9.

330. Ясенев В. Н. Информационная безопасность в экономических системах / В. Н. Ясенев. – Н. Новгород : ННГУ, 2006. – 253 с. ISBN 5-85746-736-6.

331. Abele-Wigert I. The International CIIP Handbook 2006. An Inventory of Protection Policies in 20 Countries and 6 International Organizations / I. Abele- Wigert, M. Dunn. – Zurich: Center for Security Studies, 2006. – P. 394-398.

332. Adam A. On-line leisure: gender and ICTs in the home / A. Adam, E. Green // Information, Communication and Society, 1998. – № 1(3). – P. 291-312.

333. Adam A. The Gender Agenda in Computer Ethics. Ed. Kenneth Einar Himma and Herman T. Tavani / A. Adam. – New York: John Wiley. – P. 589-621.

334. Alberts D. S. Defensive Information War: Problem Formation and Solution Approach / D. S. Alberts. – Washington: D.C. University Press, 1996. – P. 35-36.

335. Anderson R. D. Using the New ACM Code of Ethics in Decision Making / R. Anderson, D. Johnson, D. Gotterbarn, J. Perrolle // Communications of the ACM. – 1993. – №36. – P. 98-107.

336. Apresyan R. G. Ascenso a la moral / R. G. Apresyan. – Moscow: Editorial Progreso, 1991. – 286 c.

337. Are Poor Countries Losing the Information Revolution? // InfoDev Working Paper, 2000. – May.

338. Badham R. L. Theories of Industrial Society // R. L. Badham. – London: Croom Helm, 1986. – 188 p.

339. Baird R. Cyberethics: Social & Moral Issues in the Computer Age / R. Baird, R. Ramsower, S. Rosenbaum. – Amherst, New York: Prometheus Books, 2000. – 124 p.

340. Bar F. The Future of Networking / F. Bar, M. Borrus. – Berkeley, CA: University of California, BRIE Working paper, 1993. – 104 p.

341. Barlow J. A. Declaration of the Independence of Cyberspace / J. A. Barlow // Declaring Independence, 1996. - № 4.06. – W. 121-122.

342. Barnhart M. G. Nature, nurture and no-self: Bioengineering a. Buddist values / M. G. Barnhart // J. of Buddistethics. – London, 2000. – Vol. 7, № 3. – P. 126-144.

343. Bell D. The third technological revolution and its possible socioeconomic consequences / D. Bell // Dissent. – New York, 1989. – Vol. 367, № 2. – P. 165-172.

344. Benkler Y. The wealth of networks : how social production transforms markets and freedom (1st ed.) / Y. Benkler. – New Haven, Conn: Yale University Press, 2006. – 528 p.

345. Bonfield P. Changing values, the role of business in a sustainable society / P. Bonfield. – British Telecom Occasional Papers, 1998. – No. 2.

346. Britz J. Making the global information society good: A social justice perspective on the ethical dimensions of the global information society / J. Britz // Journal of the American Society for Information Science and Technology, 2008. – Vol. 59(7). – P. 1171-1183.

347. Brody R. Information ethics in the design and use of metal / R. Brody // IEEE Technology and Society Magazine, 2003. - № 22(2). – P. 34-39.

348. Bynum T. Ethical Challenges to Citizens of the Automatic Age: Norbert Wiener on the Information Society / T. Bynum // Journal of Information, Communication and Ethics in Society, 2004. – № 2(2). – P. 65-74.

349. Bynum T. Flourishing Ethics / T. Bynum // Ethics and Information Technology, 2006. – № 8(4). - P. 157-173.

350. Bynum T. How to do Computer Ethics - A Case Study: The Electronic Mall Bodensee, in J. van den Hoven (ed.), Computer Ethics-Philosophical Enquiry / T. Bynum, P. Schubert. – Rotterdam: Erasmus University Press, 1997. – P. 85-95.

351. Bynum T. Norbert Weiner and the Rise of Information Ethics, in J. van den Hoven and J. Weckert (eds.), Information Technology and Moral Philosophy / T. Bynum. – Cambridge: Cambridge University Press, 2008. – P. 19-20.

352. Bynum T. Norbert Wiener's Vision: the Impact of the 'Automatic Age' on our Moral Lives, in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives / T. Bynum. – Albany, NY: SUNY Press, 2005. – P. 11-25.

353. Bynum T. The Foundation of Computer Ethics / T. Bynum // Computers and Society, 2000. – № 30(2). – P. 6-13.

354. Bynum T. Computer and Information Ethics // The Stanford Encyclopedia of Philosophy. [Электронный ресурс]. – URL : http://plato.stanford.edu/archives/win2008/entries/ethics-computer/.

355. Capurro R. Information ethics / R. Capurro // CSI-communication, 2005. – Vol. 28. – № 12. – P. 7-11.

356. Capurro R. Information technology and technologies of the self / R. Capurro // Journal of Information Ethics, 1996. – № 5. – P. 19-28.

357. Capurro R. Informationsethos und informationsethik - Gedankenzum verantwortungsvollen handeln im bereich der fachinformation [Information ethos and information ethics - Ideas to take responsible

action in the field of information] / R. Capurro // Nachrichten für Dokumentation, 1988. – V. 39. – S. 1-4.

358. Capurro R. Intercultural information ethics / R. Capurro // Paper presented at International ICIE Symposium 2004: Localizing the Internet: Ethical issues in intercultural perspective. – Vol.4. – P. 21-38.

359. Capurro R. Moral issues in information science / R. Capurro // Journal of information science, 1985. – № 11. – P. 113-123.

360. Capurro R. Technics, Ethics, and the Question of Phenomenology / R. Capurro // In: Tymieniecka A.-T., Hrsg.: Morality within the Life- und Social World. Analecta Husserliana XXII. – Dordrecht: Reidel, 1987. – S. 475-482.

361. Capurro R. Towards an ontological foundation of information Ethics / R. Capurro // Ethics and Information Technology, 2006. – Vol. 8. – № 4. – P. 175-186.

362. Carbo T. Global information ethics: Intercultural perspectives on past and future research / T. Carbo, M. Smith // Journal of the American Society for Information Science and Technology, 2008. – № 59(7). – P. 1110-1123.

363. Cavelty M. Introduction: Securing the Homeland: Critical Infrastructure, Risk, and (In)Security / M. Cavelty, K. Kristensen. – London: Routledge, 2008. – 192 p.

364. Christians C. G. Information ethics in a complicated age / C. G. Christians // Ethics and the librarian. – 1991. – P. 3-17.

365. Connolly F. A. Call for a Statement of Expectations for the Global Information Infrastructure / F. A. Connolly // Global Information Ethics, A Special Issue of Science and Engineering Ethics. – 1996. – Vol. 2, № 2. – P. 167-190.

366. Creative Commons. [Электронный ресурс]. – URL: http://creativecommons.org/.

367. Cudd A. Objectivity and ethno-feminist critiques of science. In: K. Ashman and P. Baringer (Eds.), After the Science Wars / A. Cudd. – New York, London: Routledge, 2001. – P. 92-94.

368. DeCew J. Privacy and policy for genetic research. In: Tavani, H.T. (Ed.), Ethics, Computing, and Genomics / J. DeCew. – Sudbury: Jones and Bartlett, MA, 2006. – P. 121-136.

369. DeMaio H. B. Information ethics - It doesn't come naturally / H. B. DeMaio // Computer Security Journal. – 1988. – №5(1). – P. 7-19.

370. Dibbell J. A Rape in Cyberspace: How an Evil Clown, A Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society / J. Dibbell. – [Электронный ресурс]. – URL: http://www.juliandibbell/com/.

371. Drucker P. F. The Age of Discontinuity. Guidelines to Our Changing Society / P. F. Drucker. – London : New Brunswick (US). – 1994. – 420 p.

372. Edelstein A. Total Propaganda. From Mass Culture to Popular Culture / A. Edelstein. – Manchaster: Royal Press, 1997. – 420 p.

373. Eisenstein E. L. The Printing Press as an Agent of Change / E. L. Eisenstein. – Cambridge: Cambridge University Press, 1979. – X-XI.

374. Electronic Frontier Foundation [Электронный ресурс]. – Режим доступа : https://www.eff.org/ (дата обращения: 10.01.2012).

375. EPCglobal ратифицирует стандарт ратифицирует стандарт Gen-2 [Электронный ресурс]. – URL: http//www.rfidjournal.com/article/1293/1.

376. Eriksson J. Cyberplagues, IT, and Security: Threat Politics in the Information Age / J. Eriksson // Journal of Contingencies and Crisis Management, 2001. – Vol. 9(4). – P. 211-222.

377. Eriksson J. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State / J. Eriksson, G. Giacomello // International Studies Review, 2009. – Vol. 11(1). – P. 205-230.

378. Ethical Aspects of ICT Implants in the Human Body. Opinion No. 20 [Электронный ресурс]. – URL: http://ec.europa.eu/european_group_ethics/avis.

379. EUSIDIC [Электронный ресурс]. – URL: http://www.eusidic.org/.

380. Ferguson R. Moyen de communication de mass, education et democratie / R. Ferguson // Revue Educations. – 1997. – №14. – P. 16-20.

381. Flichy P. The Internet Imaginaire / P. Flichy London, UK, Cambridge, MA: The MIT Press, 2007. – 264 p.

382. Floridi L. Information Ethics: Its Nature and Scope / L. Floridi. – Computers and Society, 2006. – № 36(3). – P. 37-56.

383. Floridi L. Information Ethics: On the Theoretical Foundations of Computer Ethics/ L. Floridi // Ethics and Information Technology. – 1999. – №1(1). – P. 37-56.

384. Floridi L. Internet Ethics: The Constructionist Values of Homo Poieticus, in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives / L. Floridi. – Albany: SUNY Press, 2005. – P. 195-214.

385. Floridi L. Mapping the foundationalist debate in computer ethics / L. Floridi, J. Sanders // Ethics and Information Technology, 2002. – № 4. - P. 1-9.

386. Floridi L. The Foundationalist Debate in Computer Ethics, in R. Spinello and H. Tavani (eds.), Readings in CyberEthics, 2nd edition / L.Floridi, J. Sanders. – Sudbury, MA: Jones and Bartlett, 2004. – P. 81-95.

387. Flugel J. Prof. W. McDougall. 1871–1938 / J. Flugel, J. Brit // Psychol., Gen. section. – 1939. – Vol. 29. – P. 4-14.

388. Flynn E. P. Issues in medical ethics / E. P. Flynn. – Kansas City, 1997. – 384 p.

389. Foucault M. Discourse and Truth: the Problematization of Parrhesia / M. Foucault. – Berkeley: University of California, 1983. – 66 p.

390. Foucault M. The Foucault Reader, edited by P. Rabinow / M. Foucault. – New York: Pantheon Books, 1984. – P. 32-50.

391. Freeman L. Information Ethics: Privacy and Intellectual Property / L. Freeman, G. Peace. – Hersey, London: Information Science Publishing, 2005. – P. 276.

392. Froehlich T. A brief history of information ethics. Textos univerisitaris de biblioteconomia i documentació, 2004. – №13 / T. Froehlich. – [Электронный ресурс]. – URL: http://www.ub.es/bid/13froe12.htm.

393. Froehlich T. Ethical considerations of information professionals / T. Froehlich // Annual Review of Information Science and Technology, 1992. – № 27. – P. 291–324.

394. Froehlich T. Survey and analysis of legal and ethical issues for library and information services // UNESCO Report (Contract no.

401.723.4), for the International Federation of Library Associations. IFLA Professional Series. –Munich: G. K. Saur, 1997. – 97 p.

395. Garnham A. Artificial intelligence: An introd / A. Garnham. – London, New York, 1998. – 536 p.

396. Gavison R. Privacy and the Limits of the Law / R. Gavison // The Yale Law Journal, 1984. – Vol.8. – P. 421-471.

397. Goldsmith J. Who Controls the Internet?: Illusions of a Borderless World / J. Goldsmith, T. Wu. – New York: Oxford University Press, 2006. – 219p.

398. Gonnet J. Modes et permanences / J. Gonnet // Revue Educations. – 1997. – № 14. – P. 10-15.

399. Good I. J. In Communication Theory (W. Jackson, ed.) / I. J. Good. – London, Washington: Butterorth D.C., 1953. – 267 p.

400. Gorniak-Kocikowska K. The Computer Revolution and the Problem of Global Ethics, in T. Bynum and S. Rogerson (eds.), Global Information Ethics / K. Gorniak-Kocikowska. – Guildford, UK: Opragen Publications, 1996. – P. 177-90.

401. Gotterbarn D. Computer Ethics: Responsibility Regained, National Forum / D. Gotterbarn // The Phi Beta Kappa Journal. – 1991. – №71. – P. 26-31.

402. Gotterbarn D. Informatics and Professional Responsibility / D. Gotterbarn // Science and Engineering Ethics, 2001. – № 7(2). – P. 221-230.

403. Gotterbarn D. Responsible Risk Analysis for Software Development: Creating the Software Development Impact Statement / D. Gotterbarn, S. Rogerson // Communications of the Association for Information Systems. – 2005. – №15(40). – P. 730-750.

404. Gotterbarn D. Software Engineering Code of Ethics / D. Gotterbarn, K. Miller, S. Rogerson // Information Societ. – 1997. – №40(11). – P. 110-118.

405. Hague B. Digital Democracy. Discourse and Decision-Making in the Information Age / B. Hague, B. Loader. – London, New York: Routledge, 1999. – 272 p.

406. Haraway D. Simians, Cyborgs and Women: The Reinvention of Nature / D. Haraway. – London: Free Association Books, 1991. – 157 p.

407. Harris V. Archival ethics / V. Harris // IASA Journal. – 2005. – №25(5). – P. 4-12.

408. Hayashi Y. Johoka shakai: Hado na shakai kara sofuto na shakai / H. Yujiro. – Tokyo : Feo, 1969. − 189 p.

409. Hauptman P. Ethical challenges in librarianship / P. Hauptman. – New York: Oryx press, 1988. – 127 p.

410. Henkin L. Privacy and autonomy / L. Henkin // Columbia Law Review, 1974. – Vol. 77. – P. 1410-1425.

411. Himanen P. The Hacker Ethic and the Spirit of the Information / P. Himanen. – Cambridge MA, London Age: MIT Press, 2001. – 232 p.

412. Himma K. Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking, in Himma and H. Tavani (eds.). The handbook of information and computer ethics / K. Himma. – New Jersey: Wiley-Interscience, 2008. – 704 p.

413. Himma K. The Relationship Between the Uniqueness of Computer Ethics and its Independence as a Discipline in Applied Ethics / K. Himma // Ethics and Information Technology. – 2003. – № 5(4). – P. 225-237.

414. Holl S. The centrality of culture: notes on the cultural revolutions of our Time. Media and cultural regulation / S. Holl . – London: Open Univ., 1997. – 207 p.

415. Hongladarom S. Analysis and Justification of Privacy from a Buddhist Perspective / S. Hongladarom. – Information Technology Ethics: Cultural Perspectives: Idea Group, 2007. – P.108-122.

416. Huff C., D. Martin. Computing Consequences: A Framework for Teaching Ethical Computing / C. Huff, D. Martin // Communications of the ACM. – 1995. – № 38(12). – P. 75-84.

417. Human Development Report 2001. [Электронный ресурс]. – URL: http://www.undp.org/hdr2001/completenew.pdf [Geo-2-278].

418. Johnson D. Computer Ethics, 3rd ed. / D. Johnson. – New Jersey: Prentice Hall, 2001. – 240 p.

419. Kochen M. Information and society / M. Kochen // In: Williams M.E. Annual Rev. Sc. Techn. – 1983. – № 18. – P. 277-304.

420. Kocikowski A. Geography and Computer Ethics: An Eastern European Perspective, in T. Bynum and S. Rogerson (eds.) / A.

Kocikowski // Science and Engineering Ethics (Special Issue: Global Information Ethics), 1996. – № 2(2). – P. 201-210.

421. Kreie J. How men and women view ethics / J. Kreie, T. Cronan // Communications of the ACM, 1998. – № 41(9). – P. 70-76.

422. Ladd J. The quest for a code of professional ethics: an intellectual and moral confusion. In Johnson D., Snapper J., Eds. Ethical Issues in the Use of Computers / J. Ladd. – Belmont: Wadsworth, 1985. – P. 8-13.

423. Latak A. Identity Crisis: To make its players safe the NFL is tackling schemers and scammers Legal Affairs. Retrieved, 2005. February / A. Latak. – [Электронный ресурс]. – URL: http://www.legalaffairs.org.

424. Lenk H. Konnen Informationssysteme moralisch verant – wortlich sein? / H. Lenk // Informatik – Spektrum. – B. Etc. , 1998. – Bd 12, H. 5. – S. 248-245.

425. Les dimensions internationales du droit du cyberspace. Publio sous la direction de Teresa Fuentes-Camacho. – New York: Editions UNESCO, 2000. – 284 p.

426. Lessig L. Code and Other Values of Cyberspace / L. Lessig. – New York: Basic Books, 1999. – 432 p.

427. Levy S. Hackers. Heroes of the Computer Revolution / S. Levy. – Harmondsworth UK: Penguin, 1984. – 520 p.

428. Libicki M. Information Dominance / M. Libicki // Strategic Forum. – 1997. – №132. – P. 322-336.

429. Lü Y. Privacy and data privacy in contemporary China / Y. Lü // In Ethics and Information Technology. – 2005. – P. 7-15.

430. Management of government information systems, elements of strategies and policies. – New York: United Nations, 1999. – 192 p.

431. Maner W. Starter Kit in Computer Ethics / W. Maner. – Hyde Park, New York: Helvetia Press and the National Information and Resource Center for Teaching Philosophy, 1980. – 80 p.

432. Maner W. Unique Ethical Problems in Information Technology, in T. Bynum and S. Rogerson (eds.) / W. Maner // Science and Engineering Ethics (Special Issue: Global Information Ethics), 1996. – №2(2). – P. 137-154.

433. Marturano A. Genetic Information: Epistemological and Ethical Issues. In Himma K., Tavani H. (Ed.) The handbook of information and

computer ethics / A. Marturano. – New Jersey: Wiley-Interscience, 2008. – P. 385-407.

434. Masuda Y. The information society as post – industrial society / Y. Masuda. – Washington: World Future Society, 1983. – 171 p.

435. Mather K. The Theoretical Foundation of Computer Ethics: Stewardship of the Information Environment, in Contemporary Issues in Governance / K. Mather // Proceedings of GovNet Annual Conference, Melbourne, Australia, 28-30 November. – Melbourne: Monash University, 2005. – P. 146-158.

436. Mayer F. C. The Internet and Public International Law-Worlds Apart? / F. C. Mayer // European Journal of International Law (EJIL). – 2001. – Vol. 12, №3. – P. 617-622.

437. Mayer P. Das Internet im offentlichen Recht. Unter Berucksichtigung europarechtlicher und volkerrechtlicher Vorgaben / P. Mayer. – Berlin: Duncker & Humblot, 1999. – 265 s.

438. McMahon J., Cohen R. Lost in cyberspace: ethical decision making in the online environment / J. McMahon, R. Cohen // Ethics and Information technology, 2009. – Vol. 11(1). – P. 1-17.

439. McQuail D. Mass Communication and Public Interest: Towards Social Theory for Media Structure and Performance / D. McQuail // Communication Theory Today. Polity Press, 1994. – P. 241-254.

440. Metaphilosophy. – Oxford, 1985. – Vol. 16, № 4. – 318 p.

441. Mettler-Meibom B. Soziale Kosten in der Informatinonsgesellschaft: Uberlegungen zu einer Kommunilationsokologie / B. Mettler-Meibom. – Frankfurt a.M.: Fischer Taschenbuch Verl., 1987. – 121 p.

442. Moor J. Using genetic information while protecting the privacy of the soul, in Tavani, H.T. (Ed.), Ethics, Computing, and Genomics / J. Moor. – Sudbury: Jones and Bartlett, MA, 2006. – P. 109-119.

443. Moor J. What Is Computer Ethics? / J. Moor // Metaphilosophy, 1985. – №16(4). – P. 266-275.

444. Moor J. Why We Need Better Ethics for Emerging Technologies / J. Moor // Ethics and Information Technology, 2005. – Vol. 7(3). – P. 111-119.

445. Moore A. Information Ethics: Privacy, Property, and Power / A. Moore. – Seattle: University of Washington Press, 2005. – P. 297-354.

446. Morande P. Education for a responsible technology as anthropological programmer for recovering a sense of the gratuity of human life / P. Morande // Science in the context of human culture II, scientific meet., Sept.30-Oct.4, 1991. – Vatican City,1997. – P.299-311.

447. Nakada M. Japanese conceptions of privacy: An intercultural perspective / M. Nakada, T. Tamura // In Ethics and Information Technology. – 2005. – P. 27-36.

448. Negroponte N. Being Digital / N. Negroponte. – New York: Alfred A. Knopf, 1995. – 243 p.

449. Nissenbaum H. The Meaning of Anonymity in an Information Age / H. Nissenbaum // The Information Society, 1999. – № 15. – P. 141-144.

450. One Laptop per Child FAQ [Электронный ресурс]. – URL: http://laptop.org/fag.en_US.html .

451. Pfalzgraff R. L. Future War in the information Age: New Chellenges for U.S. Security / R. L. Pfalzgraff, R. H. Shultz. – London: London Print House, 1997. – 137 p.

452. Plant S. Zerosþ+Ones: Digital Womenþthe New Technoculture / S. Plant. – London: Fourth Estate, 1997. – 320 p.

453. Posner R. An economic theory of privacy / R. Posner // Regulations. – 1978. – May–June. – P. 19-26.

454. Post D. The Great Debate: Law in the Virtual World / D. Post, D. Johnson // First Monday, 2006. – Vol. 11(2). – P. 1230-1238.

455. Quoted in Noble D. Forces of Production: A Social History of Industrial Automation. – New York : Knopf, 1984. – 72 p.

456. Rattray G. Strategic Warfare in Cyberspace / G. Rattray. – Cambridge : MIT Press, 2001. – 480 p.

457. Regan P. M. Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill / P. M. Regan. – North Carolina: University of North Carolina Press, 1995. – 301 p.

458. Reidenberg J. Rules of the Road on Global Electronic Highways: Merging the Trade and Technical Paradigms / J. Reidenberg // Law & technology, 1993. – 287 p.

459. Reidenberg J. Technology and Internet Jurisdiction / J. Reidenberg // University of Pennsylvania Law Review. – 2005. – Vol.153. – P. 1951- 975.

460. Research on mitigating the insider threat to information systems. – RAND Conference Proceedings, August, 2000. – 111 p.

461. Robertson D. S. The information revolution / D. S. Robertson // Communication research. – New York, 2009. – Vol. 17, № 2. – P. 232-254.

462. Rodiger K. Informatik und Verantwortung / K. Rodiger // Informatik Spektrum. B. Etc., 1998. – Bd. 12. – H. 5. – S. 281-289.

463. Roszak T. The Cult of Information. The Folklore of computers and the True Art of Thinking / T. Roszak. – New York: Pantheon Books, 2000. – 764 p.

464. Schultz R. Contemporary issues in ethics and information technology / R. Schultz. – Hershey: IRM Press (an imprint of Idea Group Inc.), 2006. – 214 p.

465. Schwarz S. Research, integrity and privacy. Notes on a conceptual complex / S. Schwarz // Social Science Information. – 1979. – №18(1). – P. 103-136.

466. Segan S. Female of the species; hacker women are few but strong / S. Segan. [Электронный ресурс]. – URL: http://more.abcnews.go.com/sections/tech/dailynews/hackerwomen000602.html/

467. Shea V. Netiquette / V. Shea. – San Francisco: Albion Books, 1994. – 162 с.

468. Sollfrank C. Not every hacker is a woman. In: Reiche C., Sick A. (Eds.) Technics of Cyberfeminism / C. Sollfrank [Электронный ресурс]. – URL: http:www.obn.org/reading_room/writings/html/notevery.

469. Spafford E. Are Computer Hacker Break-Ins Ethical? / E. Spafford // Journal of Systems and Software, 1992. – №17. – P. 41-47.

470. Spinello R. A. Ethical aspects of information technology / R. A. Spinello. – New Jersey: Englewood Cliffs, 1995. – 226 p.

471. Spinello R. Cyberethics: Morality and Law in Cyberspace, Third Edition / R. Spinello. – Sudbury, Massachusetts: Jones and Bartlett Publishers, 2006. – 232 p.

472. Stabile C. Feminism and the Technological Fix / C. Stabile. – Manchester, New York: University Press Manchester, 1994. – 280 p.

473. Stonier T. Towards a new theory of information / T. Stonier // J. Of inform. science. – Amsterdam, 1991. – Vol. 17, №2. – P. 257-263.

474. Sudweeks F. Cultural Attitudes towards Technology and Communication / F. Sudweeks. – Murdoch: Murdoch University, 2004. – P. 385-396.

475. Szafranski R. A theory of Information Warfare. Preparing for 2020 / R. Szafranski // Airpower Journal. – 1995. – Spring. [Электронный ресурс]. – URL: http://cryptome.org/jya/af-infowar.htm#szfran.

476. Tavani H. T. Informational Privacy: Concepts, Theories, and Controversy / H. T. Tavani. – New Jersey: John Wiley & Sons, 2008. – P. 131-165.

477. Tavani H. Privacy and the Internet / H. Tavani // Proceedings of the Fourth Annual Ethics and Technology Conference. – Chestnut Hill, MA: Boston College Press, 1999. – P. 114-125.

478. Tavani H. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies / H. Tavani, J. Moor // Computers and Society, 2001. – № 31(1). – P. 6-11.

479. Tavani H. The Impact of the Internet on our Moral Condition: Do We Need a New Framework of Ethics? in R. Cavalier (ed.), The Impact of the Internet on our Moral Lives / H. Tavani. – Albany: SUNY Press, 2005. – P. 215-237.

480. Tavani H. The Uniqueness Debate in Computer Ethics: What Exactly is at Issue and Why Does it Matter? / H. Tavani // Ethics and Information Technology, 2002. – № 4(1). – P. 37-54.

481. Tavany H. Cyberethics and the future of computing / H. Tavani // Computers a. Society. – New York, 1996. – Vol. 26, № 2. – P. 22-29.

482. Taylor P. Hackers: Crime in the Digital Sublime / P. Taylor. – London, New York: Routledge, 1999. – 134 p.

483. The electronic grapevine: Rumor, reputation a. reporting in the new on-line environment. – New Jersey : Mahwah, 1998. – VI. – 199 p.

484. Turner A. J. Summary of the ACM/IEEE-CS Joint Curriculum Task Force Report: Computing Curricula, 1991 / A. J. Turner // Communications of the ACM. – 1991. – №34(6). – P. 69-84.

485. Vindg V. The Coming Technological Singularity: How to Survive in the Post-Human Era, 1993 / V. Vindg. [Электронный ресурс]. – URL: http://andrzej. virtualave/singulariti.html.

486. Warren S. Privacy, photography, and the press / S. Warren, L. Brandeis // Harvard Law Review. – Cambridge: Mass, 1891. – Vol. 4. – P. 2303-2312.

487. Watzlawick P. Die erfundene Wirklichkeit. – Munchen: Piper Verlag, 1998. – 326 p.

488. Weber M. The Protestant Ethic and the Spirit of Capitalism / M. Weber. – London: Routledge, 1930. – 271 p.

489. Westin A. Privacy and Freedom / A. Westin. – New York: Atheneum Press, 1967. – 487 p.

490. Wiener N. Cybernetics: or Control and Communication in the Animal and the Machine / N. Wiener. – New York: Technology Press/John Wiley & Sons, 1948. – 360 p.

491. Wiener N. The Human Use of Human Beings: Cybernetics and Society / N. Wiener. – Boston: Houghton Mifflin; Second Edition Revised, New York: Doubleday Anchor, 1954. – 344 p.

492. Wisconsin Bans Forced Human Chipping // Free Market News Network, 2006. – 1 June. – 24 p.

493. Youm K. H. Who Controls the Internet? Illusions of a Borderless World (Book Review) / K. H. Youm // Journalism and Mass Communication Quarterly, 2006. – Vol. 83(3). – P.730–734.

494. Yukio T. The dominance of English and Linguistic discrimination / T. Yukio // Media Development. – New York, 1992. – 192 p.

495. Zittrain J. Internet Points of Control. In S. Braman (ed.), The Emergent Global Information Policy Regime / J. Zittrain. – Houndmills: Palgrave, 2004. – P. 62-85.

ОГЛАВЛЕНИЕ

Научное издание

Дари Шойбоновна Цырендоржиева,
доктор философских наук, профессор

Оксана Михайловна Манжуева,
доктор философских наук, доцент

ФЕНОМЕН ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Монография

Текст печатается в авторской редакции

Подписано в печать 08.06.2020. Формат 60х84 1/16.
Усл.-печ. л. 17,9. Уч.-изд. л. 12,24. Тираж 500. Заказ 76
Цена договорная

Издательство Бурятского госуниверситета
670000, г. Улан-Удэ, ул. Смолина, 24 а
e-mail: riobsu@gmai

Отпечатано в типографии
Издательства Бурятского госуниверситета
670000, г. Улан-Удэ, ул. Сухэ-Батора, 3