УДК 004.056
DOI: 10.18101/978-5-9793-1397-9-97-100

НЕКОТОРЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

© **Цыбикова Туяна Сандаликовна**
кандидат педагогических наук, доцент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: cts2001@mail.ru

В настоящее время развитие человеческой цивилизации переходит на новый этап, когда информация становится важным ресурсом, а ее потери могут обернуться неприятными последствиями. В данной статье рассматриваются проблемы, связанные с зависимостью человека и всех сфер его деятельности от информации, защитой информации в России, зависимостью нашей страны от импорта информационных технологий (компьютерной техники и программного обеспечения), а также вопросы информационной безопасности.

Ключевые слова: информация; защита информации; информационная безопасность; программное обеспечение; импортозамещение; методы защиты информации; информационные сети; информационные технологии.

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Сегодня информация рассматривается как стратегический ресурс развития человечества. С этой точки зрения она может быть достоверной и актуальной, новой и устаревшей, но ее нельзя передавать, принимать или хранить в чистом виде. У любой информации имеется свой носитель, и передача происходит по различным каналам связи. В общем понимании информация — это результат отражения и обработки в человеческом сознании многообразия окружающего мира, это сведения об окружающих человека предметах, явлениях природы, деятельности других людей и т. д. [1, с. 12]. Фраза Н. Ротшильда «Кто владеет информацией, тот владеет миром», ставшая крылатой, показывает, что тот, кто первым получает информацию, обладает огромным преимуществом перед другими людьми, поскольку может ее использовать в своих интересах, в том числе и преступных. Например, получив конфиденциальные данные конкурента, предприниматель может улучшить финансовое благополучие своей компании. Поскольку всегда есть люди, которые хотят получить ценную информацию незаконным путем, возникает необходимость в ее защите. Таким образом, в современном обществе на первый план выходит проблема защиты информации, обеспечения ее целостности, достоверности и доступности.

В Российской Федерации сформирована и совершенствуется нормативно-правовая основа обеспечения информационной безопасности, приняты законы, регламентирующие общественные отношения в этой сфере, про-

должается разработка механизмов их реализации. Одним из основных правовых документов, обеспечивающих информационную безопасность в стране, является утвержденная Президентом РФ в сентябре 2001 г. Доктрина информационной безопасности Российской Федерации. 5 декабря 2016 г. была утверждена новая редакция доктрины, в которой представлена позиция государства в отношении актуальных задач по обеспечению информационной безопасности России. Согласно Закону о безопасности и Концепции национальной безопасности РФ, под информационной безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере[1]. Для обеспечения информационной безопасности государством постоянно ведется борьба против внутренних и внешних угроз информационному пространству нашей страны. Были сформулированы базовые принципы информационной безопасности: конфиденциальность, целостность и доступность [2, с. 13].

- Конфиденциальность — свойство нераскрытости и доступности информации без соответствующих полномочий, т. е. информация не может быть доступна или раскрыта неавторизованной стороне.

- Целостность — свойство противостоять несанкционированной модификации, это означает, что информация не подвергается никакому воздействию со стороны неавторизованного объекта.

- Доступность — возможность использования данных согласно предъявленным полномочиям.

При реализации данных принципов информационной безопасности государства были выявлены наиболее уязвимые для возможных нарушений сферы:

- системы государственного управления;
- информационные сети;
- банковские и финансовые институты;
- система обороны;
- специальные структуры.

Именно для этих государственных структур требуются специальные меры безопасности, так как ими обеспечивается суверенитет государства. Основными мерами обеспечения информационной безопасности являются средства шифрования.

Основной проблемой обеспечения информационной безопасности является защита самой информации. Государство должно обеспечить защиту информации на законодательном уровне, но на практике это, к сожалению, не работает. Исследования за первое полугодие 2018 г. показывают, что часто виновниками утечек информации являются сотрудники — настоящие

[1] Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета. 2016. 6 дек.

(53,5%) или бывшие (1,9%)[1]. Это позволяет сделать вывод о том, что безопасность информации зависит от соблюдения конфеденциальности сотрудниками больше, чем от других факторов.

В России широко используется иностранное программное и аппаратное обеспечение, это также способствует возникновению проблемы защиты информации. Е. А. Разумовская считает, что «в сфере информационных технологий России накапливаются еще более серьезные проблемы — это значительная, десятилетиями складывающаяся импортозависимость страны в компьютерной области» [3, с. 117]. Не исключено, что иностранные производители средств информатизации могут внедрять в свои продукты недекларированные возможности, которые в дальнейшем позволят злоумышленникам модифицировать или украсть ценную информацию. Все предприятия, заводы, банки в нашей стране работают на лицензионном программном обеспечении, выпускаемом за рубежом. Например, российские банки зависят от системы международных банковских переводов Swift, работают с платежными системами Visa и Mastercard и т. д. В 2014 г. Россия столкнулась с ситуацией, когда были введены ограничения при работе с системой Swift. Поэтому власти России задумались о поддержке отечественного программного обеспечения и был создан собственный аналог системы Swift — Сервис по передаче финансовых сообщений. Это будет способствовать обеспечению безопасности информации о клиентах банков, расчетах, транзакциях и т. д. С 1 января 2016 г. в России начался курс на импортозамещение в сфере информационных технологий. Согласно отчету Минкомсвязи за 2018 г., доля отечественного программного обеспечения увеличилась с 20% (в 2016 г.) до 65%[2].

Сейчас невозможно представить жизнь человека без информационных технологий — это социальные сети, интернет-магазины, мессенджеры, онлайн-банкинг. Использование всех этих приложений предусматривает добровольное предоставление пользователями различного рода персональной информации: идентификационной, визуальной и прочей. Информация пользователей при этом физически хранится на сервере корпорации, например, Google в США. Соответственно, личные данные российских пользователей, служебные, производственные, военные тайны и секреты остаются без защиты.

Таким образом, вопросы безопасности информации должны решаться не только на государственном уровне, но и отдельными пользователями и предприятиями. Для этого применяются достаточно простые, но эффективные комплексные меры:

- административные (надлежащее руководство);

[1] Глобальное исследование утечек конфиденциальной информации в первом полугодии 2018 г. [Электронный ресурс]. URL: https://www. infowatch.ru/report2018_half (дата обращения: 01.06.2019).

[2] Реальности импортозамещения в России: достижения, проблемы и решения // Информационная безопасность. 2019. № 1. С. 18–23.

- процедурные — убеждение работников в необходимости повышения защиты информации;

- законодательные — создание законодательства и контроль со стороны государства за уровнем информационной безопасности;

- программно-технические — использование отечественного программного обеспечения и информационных технологий.

На современном этапе развития общества адаптация традиционных мер защиты информации, повышение качества сбора оперативной информации, различные сетевые решения, анализ и моделирование угроз, повышение уровня знаний в области информационной безопасности создают условия для безопасного и эффективного использования информации в режиме реального времени.

Литература

1. Васильков А. В., Васильков И. А. Безопасность и управление доступом в информационных системах : учеб. пособие. М. : Инфра-М, 2017. 368 с.

2. Информационная безопасность и защита информации: учеб. пособие / Ю. Ю. Громов [и др.]. 2-е изд., перераб. и доп. Старый Оскол : ТНТ, 2016. 384 с.

3. Разумовская Е. А. Некоторые проблемы безопасности России в сфере информационных технологий // Российский журнал правовых исследований. 2016. № 1. С. 117–120.

SOME PROBLEMS OF INFORMATION SECURITY
IN MODERN SOCIETY

Tuyana S. Tsybikova
Cand. Sci. (Education), A/Prof.,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: cts2001@mail.ru

At present, the development of human civilization is entering a new stage — the information society, where the status of information is fundamentally changing. Information today is an important resource, the loss of which is fraught with unpleasant consequences. This article discusses the problems associated with the dependence of a person and all areas of his activity on information and information protection. The main problems of information security in Russia are considered. The problems associated with Russia's dependence on the import of information technology (computer hardware and software) and how it all relates to information security.

Keywords: information; information protection; information security; software; import substitution; information protection methods; information networks; information technology.