

Научная статья  
УДК 004.056.5-053.5(517.3)  
DOI 10.18101/978-5-9793-1869-1-201-211

## ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ МОНГОЛИИ

© Хатанболд Ойдов

Ph.D., заведующий отделом, ведущий научный сотрудник  
khataboldo@mas.ac.mn

© Энхчимэг Батхишиг

МА, научный сотрудник  
enkhchimeg\_b@mas.ac.mn

Институт философии Академии наук Монголии  
Монголия, 211238, г. Улан-Батор, ул. Баруун Сэлбэ, 15

В век информационных технологий цифровизация продолжает развиваться стремительными темпами. В связи с этим информационная безопасность становится актуальной, особенно для молодежи, как главного потребителя и актора Интернета и цифровых технологий. Хотя понятие безопасности имеет разное значение для разных людей, различные подходы к концепции безопасности, широкие или узкие, можно свести к общему значению безопасности: для традиционной безопасности — это защита государства; для безопасности человека — защита личности. Так, безопасность можно разделить на два основных измерения: традиционное и человеческое измерение. В статье рассматривается второе измерение, т.е. безопасность можно определить как свободу от всякого рода угроз существованию и выживанию государства, человеческого рода и других живых существ. Статья базируется на данных предварительных исследований конца 2022 г. «Социальные риски молодежи в контексте дигитализации» в г. Улан-Батор (Монголия). Целью этой статьи является рассмотрение ситуации информационной безопасности, вызванной активным использованием социальных сетей среди молодежи, являющихся одними из основных пользователей в быстро меняющемся процессе перехода к цифровым технологиям. Выявлено, что все чаще молодые люди получают информацию в основном из Facebook и Instagram, меньше смотрят телевизор и проводят слишком много времени в Интернете. Сделаны выводы о том, что отсутствует защита граждан от риска подвергнуться киберпреступности, а также оперативное и надежное решение данного вопроса.

**Ключевые слова:** безопасность, молодежь, цифровизация, интернет, социальные сети.

**Благодарности:** Благодарность авторов исследовательской группе, работающей над совместным грантом Фонда науки и технологии Монголии и Белорусского ФФИ, ШУТ ХТБ-2022/01-“Социальные риски молодежи Беларуси и Монголии в контексте дигитализации” в Монголии Улан-Баторской школе под руководством доктора социологических наук (Ph.D), ассоциативного профессора Цэцэнбилэг Цэвээний. Статья подготовлена при поддержке совместного гранта Фонда науки и технологии Монголии и Белорусского ФФИ, ШУТ ХТБ-2022/01-“Социальные риски молодежи Беларуси и Монголии в контексте дигитализации”.

### Введение

Феномен цифровизации является знаковым, определяющим первые 20 лет XXI века, и связан с обновлением всех систем общественных отношений при пе-

реходе на новый этап развития под ее влиянием. В результате этого процесса существенно обновляются социальная структура, отношения, ценностные ориентации, система повседневного образа жизни. По мере того, как молодые люди становятся наиболее активными агентами цифрового потребления в процессе образования и взросления, они неизбежно ощущают на себе как возрастание степени опасностей и рисков, так и их видов. В связи с этим возникает необходимость всестороннего изучения цифрового потребления современной молодежи и ее информационной безопасности.

Для Монголии начало использования Интернета датируется 1994 годом, когда ООО «Информационные коммуникации», ныне ООО «Датаком» запустило услуги электронной почты и сетевые подключения, а затем 17 января 1996 г. они были подключены к круглосуточной сети Интернет. В то время было более 500 зарегистрированных пользователей Интернета, через 28 лет прошедших с тех пор, на 2022 год 84,3% от общей численности населения пользуются Интернетом. (Г.Билгүдэй, 2022)

Активная цифровизация общества ведет к реформам и изменениям, с одной стороны упрощая деятельность людей путем замещения традиционных базовых понятий и технологий, с другой — стало необходимо учитывать безопасность общества и человека из-за инноваций и развитием технологий, что поднимает проблему информационной безопасности. В эпоху цифрового перехода должна быть сформирована нормативно-правовая база, и в этом контексте обязательно обсуждается информационное право. Информационное право — инновационная правовая концепция, набирающая обороты в области правоповедения в смысле определения прав и обязанностей сторон, участвующих в обмене современными новостями и информацией (Ч.Ганбат, 1999, хууд. 14).

Целью этой статьи является рассмотрение ситуации информационной безопасности, вызванной активным использованием социальных сетей среди молодежи, являющихся одними из основных пользователей в быстро меняющемся процессе перехода к цифровым технологиям.

#### **Методология**

В данной статье описываются предварительные результаты исследования социальных рисков молодежи от 18 до 32 лет. Анализ документов, количественные и качественные методы социологического исследования были использованы для изучения социальных рисков цифровизации среди монгольской молодежи. При этом опрос проводился методом равной выборки среди 7 основных районов города Улан-Батора. В статье рассматриваются результаты предварительных исследований районов Баянгол, Чингэлтэй и Сухэ-Баторского, в каждом районе было опрошено по 83 человек, итого 249 молодых людей в возрасте 18-32 лет методом F2F интервью.

В статье обсуждается первичные результаты опроса и анализа глубинных интервью. При этом будут рассматриваться средства и источники получения информации и информационной безопасности. Вначале поясним основные понятия и концептуальный подход исследования.

Безопасность относится к тому, что делается для защиты человека, здания или страны от опасности или преступления (Longman Dictionary of Contemporary English, 2005) Безопасность обеспечивает форму защиты, при которой создается разделение между активами и угрозой (ISECOM, 2014). Этими «активами» мо-

жет быть что угодно, например человек, место жительства, сообщество, предмет, нация или организация.

По мнению Болдуина «безопасность» может быть определена двумя конкретными вопросами: безопасность для кого? Безопасность каких ценностей? (Baldwin, 1997). Таким образом, безопасность может быть для государства, человека или международной системы (кого), а также для физической безопасности, экономического благосостояния, автономии или психологического благополучия (ценности).

Малек (2003) определяет безопасность как ценность и/или обслуживание системы с течением времени, а также отсутствие угроз для нее, после изучения природы термина «безопасность», задаваясь вопросом, было ли это целью, концепцией, дисциплина, предметная область или исследовательская программа (Malec, Security Perception: Within and Beyond the Traditional Approach., 2003). Малек предложил свое определение безопасности, что это реальное или воспринимаемое состояние, когда угроз нет, или когда существующие угрозы не представляют опасности для рассматриваемого объекта. По его мнению, это определение имеет два основных преимущества перед другими определениями безопасности:

I. Он охватывает все аспекты, а также относится к общему содержанию термина «безопасность» на всех уровнях и областях анализа,

II. Это не исключает возможного создания подполей в широко понимаемом контексте исследований безопасности, особенно когда возникают новые виды угроз (Malec, Security Perception: Within and Beyond the Traditional Approach., 2003)

Существует несколько подходов, начиная от классического Т.Гоббса и т. д. Так как они достаточно исследованы, мы хотели бы здесь выделить подход с позиции безопасности человека.

Подход к безопасности человека — это относительно новая область, которая бросает вызов традиционному подходу, утверждая, что ориентированный на государство взгляд реализма игнорировал людей или отдельных лиц, которые больше всего пострадали от войн. Комиссия по безопасности человека (CHS) определяет безопасность человека как *«...защиту основных свобод — свобод, составляющих суть жизни. Это означает защиту людей от критических и широко распространенных угроз и ситуаций, использование процессов, основанных на сильных сторонах и устремлениях людей, создание политических, социальных, экологических, экономических, военных и культурных систем, которые вместе дают людям строительные блоки для выживания, средств к существованию и достоинства»* (UN, 2022). Таким образом, человеческая безопасность рассматривает человека в качестве основного референта, в отличие от традиционного подхода к безопасности, которая ставит государство в качестве основного референта и концентрируется на том, как лучше всего защитить его. Акцент делается на обеспечении благополучия людей и реагировании на потребности людей в борьбе с источниками угроз. Кроме того, исследования безопасности человека направлены не только на поиск средств защиты нации от внешней агрессии, но и на защиту ее от ряда угроз, таких как загрязнение окружающей среды, болезни, бедность и так далее. Таким образом, безопасность человека охватывает многие аспекты безопасности, такие как продовольственная, информационная безопасность и так далее. Странники парадигмы безопасности человека утверждают,

что человек является надлежащим референтом безопасности, и государственная практика должна отражать это, а не сосредотачиваться на военной мощи (Tadjbakhsh, S., & Cheney, A., 2007) Они говорят, что традиционный подход к безопасности больше не актуален в эту крайне глобализированную эпоху, когда такие угрозы, как изменение климата, терроризм и бедность, превосходят межгосударственные нападения и войны. Однако это государство не может поддерживать свою безопасность без обеспечения безопасности своих граждан: без традиционной безопасности не может быть безопасности человека (Tadjbakhsh, S., & Cheney, A., 2007).

23 ноября 2001 г. Конвенция Европейского Союза № 185 «О компьютерных преступлениях» рассмотрела вопрос о криминализации действий в отношении компьютеров и их использования и классифицировала правонарушения в этой сфере на следующие 4 вида.

1. Преступления против конфиденциальности, целостности или доступа к компьютерным данным и системам;
2. Компьютер преступления, связанные с устройством ;
3. Преступления, связанные с содержанием информации;
4. Оно классифицируется как преступление, нарушающее права интеллектуальной собственности и другие права.

Для Монголии информационная безопасность юридически отражена в следующих законодательных актах: глава двадцать шестая Уголовного кодекса Монголии, Преступления против электронной информационной безопасности: незаконный доступ к электронной информации (статья 26.1); подготовка и продажа программного обеспечения и оборудования для незаконных атак на электронные информационные сети (статья 26.2); создание, использование или распространение вредоносного программного обеспечения (статья 26.3); Указаны три состава преступления. Однако сегодня особое внимание уделяется не только преступности электронной среды и электронных устройств, но и стратегии предотвращения преступлений против жизни, здоровья, политических прав и права на неприкосновенность частной жизни, которые могут быть совершены искусственным интеллектом (Ч.Нямсүрэн, Б.Мөнхдорж, 2020)

Эти ученые предупреждают, что, хотя открытый доступ к информации в Интернете полезен, часто встречаются негативные коннотации и ложная информация. Согласно этому, это указывает на то, что настало время всем относиться к этой большой проблеме Интернета критически.

В средствах массовой информации и социальных сетях с каждым днем обостряется тема исследования и смягчения последствий связанных с киберпространством социальных рисков, в том числе для молодежи. В связи с этим в статью включены некоторые результаты исследования, основанные на реальных потребностях общества. Результаты, представленные в статье, разделены на следующие две части.

- Во-первых, выяснить причины, с которыми молодые люди, являющиеся активными пользователями социальных сетей, могут столкнуться в процессе цифровизации.
- Во-вторых, рассчитать характеристики и характеристики риска использования электроники молодежью (кто и как они становятся жертвами использования электроники) и разработать превентивные меры.

Одной из главных причин развития Интернета является распространение и передача информации. В этом контексте существует риск среди тысяч молодых людей, которые хотят получать и давать информацию. По мнению Б. Цогням XXI век будет веком информации. Современное развитие невозможно представить без информации. Именно с этого времени формируется информационная коммуникация, или как предусмотрено нашей конституцией, граждане имеют право на получение достоверной информации, и для реализации этого права она начинается с акта требования, предоставления или отказа в предоставлении информации от других (Ч.Ганбат, 1999). Пока есть информационная коммуникация, будет обсуждаться информационная безопасность, и это, безусловно, важно. В наше время эта безопасность нарушена, и возникают серьезные проблемы личных прав. Эти проблемы включают покупку личной информации, рассылку приглашений молодежи из закрытых групп, попытки прямо или косвенно повлиять на мнение людей и т. д. в условиях цифрового перехода общества. Социальные риски среди молодежи проявляются в доверии, действии и взаимозависимости.

#### **Результаты исследований и обсуждение**

В последние годы мы видим, что многие отрасли расширили свою деятельность с помощью Интернета. Согласно данным Госкомстата в последнее время наблюдаются следующие тенденции в сферах электронной коммерции, информации и образования, цифровизации госуслуг (ҮСХ, 2022).

- **Электронная коммерция:** согласно опросу об использовании технологий, 30 % населения Монголии старше 15 лет совершали покупки в Интернете. Из них 16 % в местных районах и самый высокий показатель в Улан-Баторе, 34 %, занимались электронной коммерцией. 1/3 из них потратили 50-100 тыс. ₮, а 25% потратили 100-200 тыс. ₮.

- **Государственные услуги:** «E-Mongolia», унифицированное приложение для государственных услуг, в настоящее время имеет 1,9 миллиона пользователей. С момента запуска в 2020 году пользователи получили более 500 сервисов 6,1 млн. раз. Таким образом, с помощью Интернета госуслуги стали онлайн.

- **Информация и образование:** Самое большое решение проблемы доступа к образованию — это Интернет. 28 % людей ответили, что используют Интернет в сфере образования. У 98 % населения есть мобильный телефон, а у 84,3 % есть доступ к Интернету, что говорит о том, что мы на шаг ближе к сокращению образовательного неравенства.

По данным Госкомстата в первом полугодии 2022 года общий доход информационно-коммуникационной отрасли страны достиг 854,7 млрд тугриков, увеличившись на 105,1 (14,0 %) млрд тугриков по сравнению с аналогичным периодом прошлого года. Это увеличение произошло в основном за счет увеличения доходов от беспроводной связи на 62 (14,3 %) миллиарда тугриков, от проводной связи на 26,0 (28,6 %) миллиарда тугриков и от производства и передачи вещания на 14,1 (14,6 %) миллиарда тугриков.

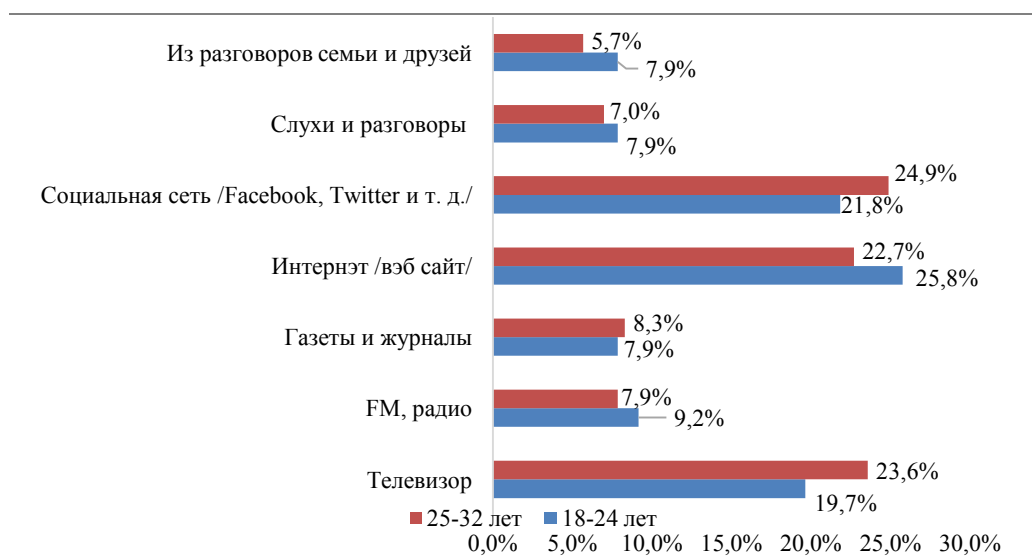
Число абонентов кабельного телевидения на конец второго квартала 2022 года достигло 975,7 тыс., что на 32,7 (3,5 %) тыс. абонентов больше, чем за аналогичный период прошлого года. Активные пользователи мобильных телефонов удвоились до 4,7 млн на конец второго квартала этого года, что на 187,8 (4,2 %) тысяч больше, чем за тот же период прошлого года. Это увеличение произошло в основном за счет увеличения на 12,8 процента в Улан-Баторе, 9,1 процента в Улан-Баторе и 2,9 процента в провинции Дундговь.

Количество интернет-пользователей достигло 4,1 млн человек на конец второго квартала 2022 года, что на 136,6 (3,4 %) больше, чем за аналогичный период прошлого года. На этот рост повлияло увеличение числа пользователей мобильного ШПД на 99,8 (2,5 %) тыс. и пользователей контрактного Интернета на 36,8 (10,7 %) тыс. соответственно.

Результаты наших предварительных данных на 3 районах г. Улан-Батора приводятся далее.

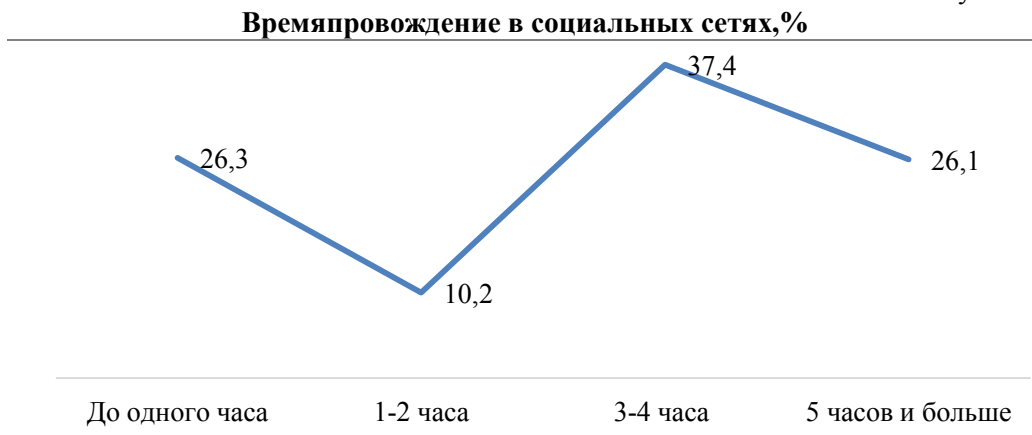
Рисунок 1

### Источники, из которых респонденты получают информацию



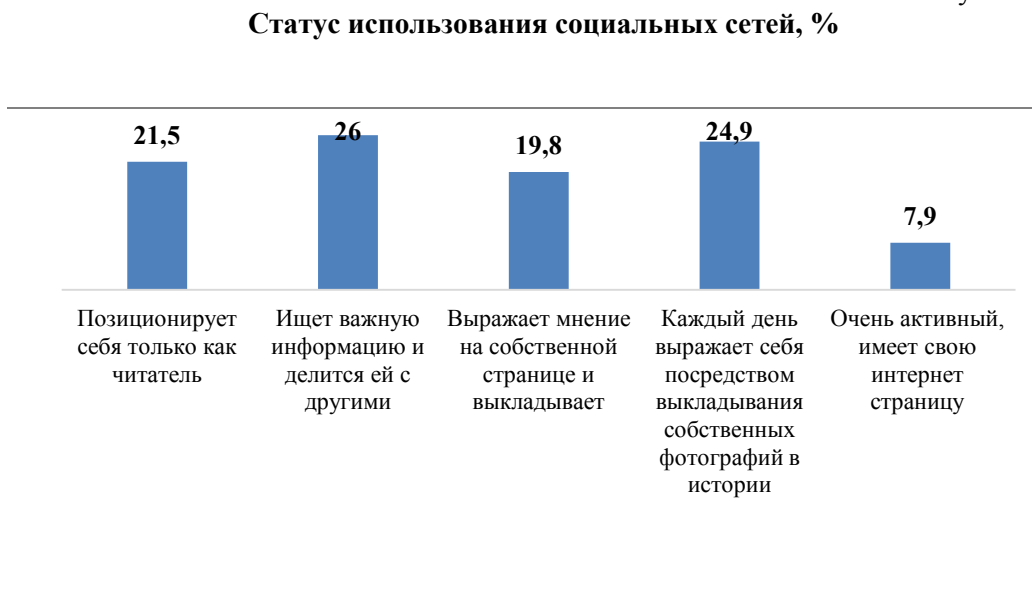
Основным источником информации для молодых людей в возрасте до 18 лет, принявших участие в опросе, является Интернет, 25,8 % — веб-страницы, 21,8 % — средства социальных сетей, 19,7 % — телевидение. Однако 22,7 % и 24,9 % молодых людей в возрасте от 25 до 32 лет получают информацию из веб-страниц и 24,9 % из инструментов социальных сетей соответственно, что Молодые люди в основном используют Facebook (31,2 %) как инструмент социальной сети. Остальные используют, Инстаграм (24,9 %), YouTube (20,8 %), Wechat (9,3 %), Twitter (7,1 %), Снэпчат (6,7 %) и т. д. 85,7 % молодых людей имеют до 1 аккаунта в Facebook и Instagram, а 14,3 % молодых людей используют от 2 до 6 аккаунтов. Однако наличие у большинства молодых людей до одного адреса может быть показателем основных принципов корректности в онлайн-среде. С другой стороны, 14,3 процента молодых людей используют 2–6 аккаунтов, а остальные 14,3 процента молодых людей открывают двойные счета и используют их только для служебной работы, так как не хотят дружить с родителями, руководителем, директором. Или руководство организации. Электронные технологии предоставляют информацию не только в виде текста и изображений, но и в виде аудио и видео.

Рисунок 2



63,4 процента опрошенной молодежи тратят более 3 часов, а 36,4 процента — 1-2 часа. Отсюда видно, что влияние электронной среды велико, а контроль за ее правильным использованием слаб.

Рисунок 3



Как видно из рисунка выше, молодым людям, участвовавшим в исследовании, свойственно искать и находить нужную им информацию и делиться ею с другими. Но другая часть, 21,5 процента, только подходит с точки зрения читателя, согласно исследованию. В опросе приняли участие 7,9 % молодых людей, имеющих очень активные личные страницы и блоги. Еще один важный вопрос — как обеспечить безопасность личной информации.

Таблица 1

**Меры, принятые для обеспечения безопасности личной информации по возрастным группам, %**

№		18-24 лет	25-32 лет
1	Смена паролей на компьютерах и сайтах онлайн-сервисов	61.7	62.4
2	Удалить историю просмотров в Интернете	40.2	41.3
3	Изменение настроек для других пользователей, которые имеют доступ к вашей информации в социальных сетях	29.0	40.4
4	Регистрация пользователей на одном компьютере	13.1	11.9
5	Удалить ненужные файлы на компьютере	26.2	25.7
6	Проверить компьютер на вирусы	12.1	13.8
7	Копия файлов, хранящихся на компьютере	12.1	6.4
8	Использование обязанностей родительского контроля на компьютере	12.1	8.3
9	Обнаружение мошеннической информации в интернет-среде	5.6	8.3
10	Уровень конфиденциальности и безопасности передачи персональной информации в интернет-среде	10.3	15.6
11	Проверить компьютер на вирусы	1.9	0.9

Более 40 % большинства опрошенных заявили, что знают, как удалить историю посещений Интернета, удалить ненужные файлы с компьютера, скопировать сохраненные файлы и проверить компьютер на наличие вирусов. В ходе опроса было выявлено, что участники не обладают определенным уровнем знаний по выявлению мошеннической информации в сети Интернет, конфиденциальности передачи личной информации в сети Интернет, проверке на наличие компьютерных вирусов и определению уровня безопасности. По мнению участников опроса, каждый десятый человек в интернет-среде имеет общую склонность к потере личной информации, к обману со стороны других или к преследованиям со стороны кого-либо. Например, тенденция обычно наблюдается среди 18–32-летних. Если его разделить по возрастным группам, 18–24-летние рискуют потерять свою учетную запись Facebook, подвергнуться влиянию или давлению и принимать запросы на добавление в друзья немедленно без какой-либо цензуры.

Причина номер один стать жертвой онлайн-мошенничества заключается в том, что люди обращаются за финансовой помощью через чаты Facebook. Но для 25–32-летних обычно запросы на добавление в друзья в Facebook принимаются только в том случае, если они дружат с кем-то, кого знают. Кроме того, если вы получите запрос на добавление в друзья на Facebook с адреса с неизвестной фотографией, вы больше не будете другом. В предыдущие годы заявки на добавление в друзья принимались, но в будущем они принимают вышеуказанные меры, чтобы защитить себя и свои семьи от будущих рисков. Кроме того, распространено явление, когда эти возрастные группы чаще обманывают других в онлайн-среде. Не следует упускать из виду, что безопасность информации включает в себя не только технические средства, но и безопасность сторон, участвующих в информационной коммуникации (Ч.Ганбат, 1999, хууд. 17).



В нашей стране с ежечасно увеличивающимся использованием компьютеров и смартфонов количество киберпреступлений увеличивается с каждым годом: в 2016 году было зарегистрировано 97, в 2017 году — 195, в 2018 году — 659, а на май 2019 года — 384 или 1335 киберпреступлений. В 2021 г. зарегистрировано 4 825 преступлений, совершенных в электронной среде, а в 2022 году — 8563, или 77,5 процента (ГБХЗХГ, 2018); (Т.Алтанзагас, 2022) В основном это женщины и несовершеннолетние, что связано с отсутствием знаний о киберпреступности и методах ее предотвращения, а также с плохим присмотром за маленькими детьми. В главе 26 специального раздела Уголовного кодекса Монголии говорится, что «в случае незаконного нападения на электронные данные, подготовки, продажи, создания, использования или распространения вредоносного программного обеспечения, программного или аппаратного обеспечения для незаконного нападения на электронные сети передачи данных налагается штраф в размере от 2 700 до 40 000 тугриков, или ограничение права передвижения на срок от 1 до 5 лет, или лишение свободы на срок от 6 месяцев до 12 лет». Установлена ответственность за киберпреступления (МУТЕГ, 2020).

### **Заключение**

Социальные сети важны в современном обществе. В настоящее время эта тема особенно актуальна для молодых людей. Знания молодежи центральных районов столицы Монголии о безопасности информационных технологий являются относительно хорошими. Риск информационных технологий напрямую связан с личной безопасностью. С развитием информационных технологий увеличилось количество рисков, что негативно сказывается на молодежи. В сфере информационной безопасности подход безопасности человека более приемлем. Для монгольского общества нельзя считать, что информационная безопасность обеспечивается только за счет хранения и защиты электронной информации. Электронные базы данных (Blockchain) и цифровая обработка сигналов (Analog) между сетями независимых пользователей также должны защищать информацию, которая реально существует. По результатам предварительных исследований видно, что отсутствует защита граждан от риска подвергнуться киберпреступности, а также оперативное и надежное решение данного вопроса. Все чаще молодые люди получают информацию в основном из Facebook и Instagram, меньше смотрят телевизор и проводят слишком много времени в Интернете. Чем больше у вас правильных знаний и отношения к использованию Интернета, тем выше вероятность того, что вы будете пользоваться Интернетом надлежащим образом. Важно обеспечить конфиденциальность и безопасность электронных новостей и информации и создать соответствующую правовую среду.

### **Литература**

1. Т. Алтанзагас. (23, 1 26). UBN. Retrieved from <https://ubn.mn/p/36991>.: <https://ubn.mn/p/36991>.
2. газар, М. у. (2020, 02 14). Монгол улсын тагнуулын ерөнхий газар. Retrieved from ОСНОВНЫЕ СВЕДЕНИЯ О КИБЕРПРЕСТУПНОСТИ: <https://gia.gov.mn/49/item/643>
3. Т. Алтанзагас. (2020, 1 26). UBN. Retrieved from 2022 онд цахим гэмт хэргийн улмаас 21.9 тэрбум төгрөгийн хохирол учирсан: <https://ubn.mn/p/36991>.
4. ФХ. (2020). Влияние электронной среды на монгольское общество: Философские вопросы (Сборник докладов научных конференций). Уб: Фх.
5. ФХ. (2020). Влияние электронной среды на монгольское общество: Философские вопросы (Сборник докладов научных конференций). Уб: Фх.

6. Улан-Баторский университет, Беларусь Национальный Институт социологии МАН. (2023). Из результатов исследования социального риска молодежи в эпоху цифровизации // Уб., 2023. Улаанбаатар.
7. Г. Билгүдэй. (2022, 02 28). Лемон пресс. Retrieved from Интернетом пользуетя 84,3% населения Монголии: [https://lemonpress.mn/news/internet\\_huduu/](https://lemonpress.mn/news/internet_huduu/)
8. ҮСХ. (2022, 12 17). ҮСХ. Retrieved from Интернет хэрэглэгч ба компьютерын тоо: <https://www2.1212.mn/>
9. Tadjbakhsh, S., & Cheney, A. (2007). Human Security: Concepts and implications (1st ed.).
10. Tadjbakhsh, S., & Cheney, A. (2007). Human Security: Concepts and implications (1st ed.).
11. Ч. Ганбат. (1999). Монгольское государство и право. Уб: Верховный суд Монголии.
12. Longman Dictionary of Contemporary English. (2005). "Security". London, England: Pearson Longman.
13. ISECOM. (2014). Open-Source Security Testing Methodology Manual (OSSTMM) (Research. Retrieved from <https://www.isecom.org/research.html>.
14. Baldwin, D. (1997). The concept of security. Review of International Studies, 23(1), pp. 5-26, doi:10.1017/S0260210597000053.
15. Malec, M. (2003). Security Perception: Within and Beyond the Traditional Approach. [https://www.researchgate.net/publication/35967961\\_Security\\_Perception\\_Within\\_and\\_Beyond\\_the\\_Traditional\\_Approach](https://www.researchgate.net/publication/35967961_Security_Perception_Within_and_Beyond_the_Traditional_Approach).
16. Malec, M. (2003). Security Perception: Within and Beyond the Traditional Approach. [https://www.researchgate.net/publication/35967961\\_Security\\_Perception\\_Within\\_and\\_Beyond\\_the\\_Traditional\\_Approach](https://www.researchgate.net/publication/35967961_Security_Perception_Within_and_Beyond_the_Traditional_Approach).
17. Ч.Нямсүрэн, Б.Мөнхдорж. (2020). Хиймэл оюун ухаан ба криминологийн хөгжлийн чиг хандлага. Влияние электронной среды на монгольское общество: Философские вопросы (р. 152). Улаанбаатар: Институт философии АНМ.
18. UN. (2022, 8 26). [www.un.org](http://www.un.org). (T. U. Security., Producer) Retrieved from Human Security in Theory and Practice: An Overview of the Human Security Concept": [www.un.org/humansecurity/files/human\\_security\\_in...](http://www.un.org/humansecurity/files/human_security_in...)
19. ГБХЗХГ. (2018). Өсвөр үеийнхний цахим хэрэглээний өнөөгийн байдал судалганы тайлан. Уб.,: Гэр бүл, хүүхэд, залуучуудын хөгжлийн газар.
20. Т.Алтанзагас. (2022). 2022 онд цахим гэмт хэргийн улмаас 21.9 тэрбум төгрөгийн хохирол учирсан. <https://ubn.mn/p/36991>. Retrieved from <https://ubn.mn/p/36991>.
21. МУТЕГ. (2020, 2 14). МУТЕГ. Retrieved from Монгол Улсын Тагнуулын ерөнхий газар: <https://gia.gov.mn/49/item/643>

#### ISSUES ON THE INFORMATIONAL SECURITY OF YOUTH IN THE CONTEXT OF DIGITALIZATION IN MONGOLIA

*Khatanbold Oidov*  
Ph.D., Head of the Department  
Leading Researcher  
[khatanboldo@mas.ac.mn](mailto:khatanboldo@mas.ac.mn)

*Enkhchimeg Bathishig*  
MA, Research Fellow  
[enkhchimeg\\_b@mas.ac.mn](mailto:enkhchimeg_b@mas.ac.mn)

Institute of Philosophy of the Mongolian Academy of Sciences  
15 Baruun Selbe St., Ulaanbaatar 211238, Mongolia

In the age of information and technology, digitalization continues to develop at a rapid pace. In this regard, information security is becoming crucial, especially for young people, as the main consumer and actor of the Internet and digital technologies. The concept of security means different things to different people. Various approaches to the concept of security, whether too broad or too narrow, discuss at least one specific aspect of security: for traditional security, it is the protection of the state; or for human security, it is the protection of the individual. All concepts of security, be it the protection of the environment or the Internet, are interconnected due to globalization, and these emerging «non-traditional» security concepts are gaining more importance than the traditional view of security. Security can be divided into two main dimensions: the traditional and the human dimension. The article uses the latter and security can be defined as freedom from all kinds of threats to the existence and survival of the state, the human race and other living beings. The article is based on data from preliminary studies at the end of 2022 titled “Social risks of youth in the context of digitalization” in Ulaanbaatar, Mongolia. The purpose of this article is to examine the situation of information security caused by the active use of social networks among young people, who are one of the main users in the rapidly changing process of digital transformation. Increasingly, young people are considered to be getting information mainly from Facebook and Instagram, watching less TV and spending too much time on the Internet. It concludes that there is no protection of citizens from the risk of being exposed to cybercrime, as well as a prompt and reliable solution to this issue.

*Keywords:* security, youth, digitalization, internet, social networks.