Научная статья
УДК 343.9+343.988
DOI: 10.47475/2311-696X-2024-42-3-80-88

С. 80–88

ВИКТИМОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Андрей Владимирович Майоров
Уральский государственный юридический университет им. В. Ф. Яковлева, Екатеринбург, Россия
ab_majorov@mail.ru
https://orcid.org/0000-0002-8629-9837

Аннотация. Информация представляет большую ценность для человека. Существует множество угроз, направленных как на безопасность информации, так и на безопасность обладателя информации. С развитием цифровых технологий проблема обеспечения информационной безопасности личности становится одной из обсуждаемых в научном сообществе. Несмотря на политику государства в сфере обеспечения информационной безопасности, а также существующие механизмы защиты информации, сохранность персональных данных пользователей остается под угрозой. Виктимологическое обеспечение информационной безопасности личности должно стать одним из эффективных методов пассивной защиты. В статье рассмотрены правовые основы виктимологического обеспечения информационной безопасности личности, основные угрозы пользователям телекоммуникационных сетей и причины возникновения опасности в информационной среде. Приведены способы виктимологической защиты цифрового профиля личности. Представленный материал является промежуточным результатом проводимого исследования по виктимологическому обеспечению безопасности цифровой личности.

Ключевые слова: информационная безопасность, информационная безопасность личности, защита информации, виктимологическая профилактика, цифровизация, цифровой профиль личности, информационная защищенность

Для цитирования: Майоров А. В. Виктимологическое обеспечение информационной безопасности личности // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 80–88. DOI: 10.47475/2311-696X-2024-42-3-80-88

Research article

VICTIMOLOGICAL PROVISIONING OF INFORMATION SECURITY OF THE INDIVIDUAL

Andrey V. Mayorov
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia
ab_majorov@mail.ru
https://orcid.org/0000-0002-8629-9837

Abstract. Information is of great value to human beings. There are many threats aimed both at the security of information and the security of the holder of information. With the development of digital technologies, the problem of ensuring personal information security becomes one of the most discussed in the scientific community. Despite the state policy in the field of information security, as well as the existing mechanisms of information protection, the safety of personal data of users remains under threat. Victimological provision of personal information security should become one of the effective methods of passive protection. The article considers the legal foundations of victimological provision of information security of the individual, the main threats to users of telecommunication networks and the causes of danger in the information environment. The ways of victimologic protection of digital profile of a person are given. The presented material is an intermediate result of the ongoing research on victimological provision of digital identity security.

Keywords: information security, information security of personality, information protection, victimological prevention, digitalization, digital personality profile, information security

For citation: Mayorov AV. Victimological provisioning of information security of the individual. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(3):80-88. (In Russ.) DOI: 10.47475/2311-696X-2024-42-3-80-88

Введение

Ни один представитель современного общества не может обходиться без цифровых и информационных технологий, с помощью которых передает и получает информацию, создает и хранит персональные данные, регистрирует права, участвует в общественных отношениях и т. д. Информационное пространство расширяется за счет цифровых технологий, в нем протекают как позитивные (цифровизация), так и негативные (криминализация) процессы.

Информация, выступая объектом публичных, гражданских и иных правовых отношений, является предметом защиты, подлежит охране со стороны государства, а также ее собственника — обладателя информации.

В процессе развития информационного общества одной из приоритетных задач для государства является обеспечение информационной безопасности граждан. Основным юридическим документом, регулирующим сферу информационной безопасности Российской Федерации, является Доктрина информационной безопасности, которая определяет информационную безопасность как «состояние защищённости личности, общества и государства от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойное качество и уровень жизни граждан, суверенитет, территориальная целостность, устойчивое социально-экономическое развитие, оборона и безопасность государства»[1].

Федеральный закон «Об информации, информационных технологиях и о защите информации» наделяет владельца информации правом на ее защиту: «обладателю информации предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информации» (ч. 4 ст. 6, ч. 1 ст. 16)[2]. При этом Конституция РФ, являясь основным источником права в сфере защиты информации, закрепляет права на неприкосновенность частной жизни, личную и семейную тайну; на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23); свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29); запрещает без согласия лица сбор, хранение, использование и распространение информации о его частной жизни (ст. 24)[3].

Уголовное законодательство РФ предусматривает ответственность за нарушение информационных прав личности, тем самым реализует охрану прав граждан (ст. 137, 138 УК РФ) и гарантирует обеспечение информационной безопасности личности (ст. 272, 274 УК РФ)[4].

Несмотря на существующую обязанность государства по защите информационной безопасности личности [2], при противоправных деяниях, посягающих на информационную безопасность, высокий уровень виктимности граждан сохраняется. Использование цифровых технологий в преступных целях привело к повышению уязвимости всех представителей общества. К наиболее уязвимой группе риска относятся лица, чьи персональные данные нуждаются в защите: государственные служащие, владельцы недвижимости, юридические лица, вкладчики банков, граждане, пользующиеся банковскими картами и др.

Согласно данным компании Statista[5], в 2023 году зарегистрировано более 3 тысяч утечек данных, которые затронули 353 миллиона человек. При этом крупные утечки, произошедшие в период с 2016 по 2019 год, содержали от 1,5 до 2,5 миллиарда личных данных. Украденные базы содержат личную информацию о владельцах учетных записей: электронную почту, пароли, адреса и данные банковских карт[6]. Именно их используют злоумышленники для кражи «цифровой личности»[7] разными способами. Несмотря на осведомленность большинства потенциальных жертв, а главное известность и распространенность мер пассивной виктимологической защиты, уровень цифровой виктимности остается высоким в силу пренебрежения цифровой гигиеной (кибергигиеной). Цифровая гигиена — это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности[8].

Материалы и методы

В качестве материалов для проведения данного исследования использованы: научные труды по проблематике и нормативные правовые акты, регулирующие сферу обеспечения информационной безопасности личности; сведения, опубликованные в открытых источниках о способах совершения и защиты от преступлений,

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «Гарант». URL: https://base.garant.ru/71556224/ (дата обращения: 12.04.2024).

[2] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.04.2024).

[3] Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 года (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 20.04.2024).

[4] Уголовный кодекс Российской Федерации : от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 12.04.2024).

[5] Statista — немецкая компания, специализирующаяся на рыночных и потребительских данных. Компания предоставляет статистические данные и результаты опросов, которые представлены в виде диаграмм и таблиц. Его основными целевыми группами являются бизнес-клиенты, преподаватели и исследователи. URL: https://www.statista.com/ (дата обращения: 20.04.2024).

[6] См.: Шувалова М. Цифровая безопасность личности: что изменилось за последний год // СПС «Гарант». URL: https://www.garant.ru/article/1528258/ (дата обращения: 20.04.2024).

[7] Цифровая личность — это портрет человека в интернете, его публичная и конфиденциальная информация. Структура цифровой личности включает в себя три основных элемента: цифровой профиль, цифровой образ и цифровой след [13, с. 20].

[8] См.: Цифровая гигиена поможет обеспечить безопасность в сети // Kaspersky. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-hygiene-habits (дата обращения: 20.04.2024).

совершаемых с использованием информационно-телекоммуникационных технологий, компьютерной информации и средств связи, посягающие на информационную безопасность личности.

Основу исследования составили общенаучные и частнонаучные методы познания, такие как анализ и синтез, индукции и дедукции, метод контент-анализа и др.

Описание исследования

В современном мире информация для человека представляет собой определенную ценность. Как и любую другую ценность, информацию стоит защищать от ее неправомерного искажения или несанкционированного доступа к ней с последующим похищением и использованием.

Для защиты данных от утечки, хищения или, например, взлома программы или компьютерной системы в современной реалии есть отрасль, которая называется информационная безопасность. Информационная безопасность — есть сфера деятельности, которая постоянно растет и развивается, которая включает обширный спектр отраслей, от безопасности сети и инфраструктуры вплоть до тестирования, а также аудита [3, с. 45].

Информационная безопасность включает в себя инструменты и процессы, которые применяют для защиты информации. Защита информации — это «организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий» [1, с. 34]. Средствами защиты информации называют устройства, приборы, приспособления, программное обеспечение, организационные меры, которые предотвращают утечку информации и обеспечивают ее сохранение в условиях воздействия всего спектра актуальных угроз.

Так, например, под информационной безопасностью личности с учетом статических и динамических характеристик предложено понимать «состояние защищенности личности, характеризуемое, с одной стороны, ее способностью противостоять внутренним и внешним информационным воздействиям, а с другой стороны — способностью информационного государства и информационного общества эффективно решать задачи по обеспечению информационной безопасности личности» [8, с. 32].

Таким образом, личность выступает в качестве объекта правового обеспечения информационной безопасности и одновременно — субъекта, участвующего в обеспечении информационной безопасности.

На криминолого-виктимологический подход в обеспечении информационной безопасности личности указывает и упомянутая выше Доктрина информационной безопасности Российской Федерации, которая среди основных направлений обеспечения информационной безопасности закрепляет такие, как «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям; обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности»[1]. Полагаем, что одним из ключевых направлений в обеспечении информационной безопасности личности должна стать виктимологическая защита потенциальных жертв в пассивной и активной форме.

Для подтверждения высказанной гипотезы рассмотрим одно из вводимых в доктрину понятий, которое в будущем возможно и будет использоваться в уголовном законодательстве — «цифровой профиль личности».

Цифровая личность

Если обратится к анализу статистики преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, то можно говорить о высоком уровне виктимизации цифрового общества. В 2020 г. МВД России зафиксировало взрывной рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации 510 396 (+73,4 %), в 2021 г. число таких преступлений увеличилось незначительно — на 1,4 % — и составило 517 722 преступления, в 2022 г. — 522 065 (+0,8 %), в 2023 г. — 676 951 (+29,7 %)[2]. При этом значительную часть преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, составляют кражи и мошенничества. Но стоит отметить, что в первую очередь для совершения указанных преступлений злоумышленникам необходима какая-либо информация о потенциальной жертве, сбор и получение которой, как правило, происходит не законными способами, с нарушением информационной безопасности личности.

С развитием информационных и цифровых технологий, появлением новых гаджетов и онлайн-сервисов растет число пользователей сети Интернет, мобильных приложений и социальных сетей. Стать пользователем не сложно, но для этого необходима регистрация на сайте. Оцифрованный набор данных о человеке — имя и фамилия, фотографии и подписи к ним, интересы и увлечения — позволяет создать цифровой профиль личности. «Цифровой профиль — наиболее важная часть цифровой личности, представляющая собой совокупность персональных и иных связанных с ними данных индивида в виртуальном пространстве, содержащихся в информационных базах уполномоченных на их обработку субъектов. С учетом этого инфраструктуру цифровой личности предлагается отнести к критической информационной инфраструктуре, которая должна соответствовать всем требованиям информационной безопасности» [12, с. 6; 13, с. 20]. Данные цифрового профиля, полученные из открытых источников, используют для

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646.

[2] См. Состояние преступности // Официальный сайт МВД РФ. URL: https://мвд.рф/folder/101762 (дата обращения: 20.04.2024).

социальной инженерии. Социальная инженерия — это метод манипуляции людьми с целью получения их конфиденциальной информации, доступа к ресурсам или других представляющих ценность объектов[1]. Социальная инженерия является противоправным методом, если используется злоумышленниками для сбора информации в преступных целях.

Рассмотрим, в чем же негативные последствия такого метода сбора информации.

Социальная инженерия

Исследованию негативных методов социальной инженерии в последнее время уделяется особое внимание со стороны представителей наук криминального цикла. В одной из таких работ автор утверждает, что «социальная инженерия в настоящее время относится к самым распространенным методам совершения противоправных деяний с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» [15, с. 475]. Другой исследователь — Е. В. Никитин — говорит о том, что «социальная инженерия позволяет преступникам повышать „эффективность“ своей вредоносной деятельности, делая потерпевших невольными помощниками своих преступлений. Находясь под воздействием технологий „социальной инженерии“, жертва внешне „добровольно“ сообщает нужную преступникам информацию, передает имущество, переводит денежные средства, участвует в выгодной преступной организации противоправной и антиобщественной деятельности и т. д.» [9, с. 486]. Для кражи цифрового профиля личности злоумышленнику не нужно быть хакером, достаточно войти к жертве в доверие, заставить ее выполнить определенное действие: отправить свои фотографии, назвать дату рождения, перейти по вредоносной ссылке. Это происходит как при живом общении, так и в переписке, например, при рассылке фишинговых писем, которые ведут на сайт-подделку или содержат вредоносную программу[2].

Одним из самых распространенных способов социальной инженерии является дистанционное — телефонное мошенничество [15, с. 478]. Согласно докладу в рамках деловой сессии «Телефонное мошенничество в России», с января по март 2024 года только телефонным мошенникам удалось похитить со счетов онлайн-банков 4 миллиона рублей[3].

Механизм совершения дистанционного мошенничества с использованием мобильной связи и меры противодействия такому преступлению становится предметом для исследования не только ученых, но и практиков. Мобильные средства связи выступает элементом системы взаимодействия во взаимосвязи «преступник — жертва». При этом, как правило, преступник обладает определенной информацией о личности потенциальной жертвы (фамилия, имя, место работы и т. п.). Целью преступника при звонке потенциальной жертве является психологическое воздействие. Так, например, И. И. Евтушенко выделяет три этапа виктимизации телефонного мошенничества: «испуг» (злоумышленник ставит потерпевшего в тупик), «снятие денег» (потерпевшему предлагается перевести деньги на безопасные счета или заблокировать доступ к личному кабинету путем сообщения индивидуального одноразового кода, приходящего на телефон), «вывод денег» [6, с. 48].

Многие сотрудники государственных и образовательных организаций столкнулись с таким видом мошенничества, когда от имени руководителя организации или его заместителя поступают адресные сообщения на различные мессенджеры с просьбой оказать срочную финансовую помощь или поддержку с последующей компенсацией. Новых технологии позволяют моделировать цифровой профиль пользователя и использовать его для преступных целей. Для подмены личности мошенниками используются: программная имитация голоса при голосовой идентификации, Deepfake — методика синтеза изображения, реализуемая с помощью искусственного интеллекта (ИИ) при идентификации клиента по изображению или видео [4, с. 95; 10; 11].

Обеспечению информационной безопасности уделяется особое внимание кредитными организациями и органами власти. За счет разработки программных средств распознания противоправных деяний расширяются технические средства виктимологической защиты от дистанционных мошенничеств. В частности, СберБанк совместно с компанией АктивБизнесКонсалт разработал специальную функцию собственного оператора сотовой связи «СберМобайл», который с помощью искусственного интеллекта анализирует текст разговора и предупреждает пользователя о подозрении на мошенничество в процессе разговора. Данная система получила название «Аура» и является самообучающейся языковой нейросетевой моделью глубокого обучения, способной распознавать меняющуюся методику мошеннического обмана потерпевшего на основании тысяч разговоров настоящих мошенников. Банк «Тинькофф» предлагает своим клиентам установить приложение, которое аналогичным образом будет отслеживать содержание разговоров с клиентом, сравнивать источник звонка и номер телефона с уже имеющейся в базе банка картотекой мошеннических номеров. «Яндекс» предлагает устанавливать на свои смартфоны онлайн определитель номера, который анализирует источник звонка, сравнивает с имеющейся базой данных телефонных номеров и сообщает владельцу, что это возможно мошенники, реклама или иной нежелательный звонок [5, с. 82].

Преступные манипуляторы тонко чувствуют человека, подбирая легенду взаимодействия под психологические особенности потенциальной жертвы и вводя ее в нужное для совершения преступления эмоциональное состояние [9, с. 489].

[1] См.: Что такое социальная инженерия? // Kaspersky. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 20.04.2024).

[2] См.: Защита цифровой личности // Репутация Москва. URL: https://reputation.moscow/2021/02/16/czifrovaya-bezopasnost-lichnosti/ (дата обращения: 20.04.2024).

[3] Там же.

Анализируя опубликованные в открытом доступе данные и результаты проводимых исследований, можно выделить три основных метода социальной инженерии:

1) угрозы, сопряженные с использованием средств телефонии (мобильных, стационарных телефонов);

2) угрозы с использованием информационной телекоммуникационной сети Интернет (электронная почта, мессенджеры, социальные сети);

3) угрозы, сопряженные с непосредственным контактом с носителем информации (сбор информации из открытых источников, плечевой серфинг, обратная социальная инженерия).

Пользователи постоянно становятся мишенями злоумышленников, и им требуется обладать достаточными знаниями, чтобы выявлять такие атаки и избегать их. Средства связи и коммуникации, а также все точки доступа, которые мы используем (например, социальные сети, интернет-магазины, онлайн-банки, мессенджеры), потенциально очень уязвимы [14].

Основными причинами утечки информации специалисты в области ее защиты, как правило, называют:

— простые пароли, выбранные пользователями, или пароли совместно используемые;

— использование методов социальной инженерии, в первую очередь фишинга, когда злоумышленники рассылают сообщения, выдавая себя за представителя другого лица, часто с целью кражи учетных данных пользователя;

— взломанные учетные записи — часто используют для получения доступа к другим, более защищенным системам;

— инсайдерские угрозы — злоумышленник может использовать свое положение для получения несанкционированного доступа к системам компании;

— вредоносное ПО — использует ботнеты для получения несанкционированного доступа к финансовым системам путем кражи учетных данных, банковской информации и финансовых данных.

По мнению специалистов и исследователей, типичное нарушение безопасности происходит в три этапа: 1) исследование — злоумышленник ищет слабые места или уязвимости в организационных системах, людях или процессах; 2) сетевая / социальная атака — злоумышленник пытается проникнуть за периметр сети либо обходя сетевые защитные системы, либо используя социальную инженерию, чтобы обманом заставить людей предоставить доступ, данные или учетные данные; 3) эксфильтрация — как только злоумышленнику удается получить доступ, он может украсть ценные активы или нанести ущерб в точке проникновения, а также осуществить боковое перемещение для получения доступа к другим, более ценным системам [7, с. 326–327].

Для предупреждения утечки информации и ее сохранности пользователю достаточно прибегнуть к пассивным методам защиты информации, что позволит избежать несанкционированного доступа к ней. Активные методы защиты необходимы уже тогда, когда происходит непосредственное посягательство или существуют реальные риски завладения информацией. К пассивным методам защиты информации можно отнести обязанность правообладателя соблюдать определенные правила и цифровую гигиену. Совокупность существующих способов и рекомендаций по защите информации от преступных посягательств можно отнести к виктимологической профилактике.

Заключение

Несмотря на предпринимаемые государством меры в сфере обеспечения информационной безопасности личности, безопасность цифрового профиля личности остается одним из проблемных аспектов.

Жертвы сами помогают преступникам, пренебрегая правилами цифровой гигиены. Пока со стороны государства не будет выработан механизм эффективной защиты цифрового профиля личности, ответственность за информационную безопасность лежит на плечах самих пользователей. Ведь большинство виктимологических ситуаций связаны с наличием у преступника доступа к базам данных различных организаций, к персональным данным о потерпевшем, его фотографиям, служебной и личной информации, переписке в рабочих «чатах» различных мессенджеров.

Одним из способов предотвращения негативных последствий в информационной среде является цифровая гигиена, которая входит в систему виктимологической профилактики как пассивный метод обеспечения безопасности цифрового профиля личности. Развитие критического мышления и осознанности помогают личности не поддаваться на манипуляции и принимать взвешенные решения, противодействуя методам социальной инженерии и дистанционным мошенничествам.

Некоторые способы обеспечения информационной безопасности личности представлены в Приложении А.

Список источников

1. Аль-Аммори А., Дяченко П. В., Клочан А. Е., Бакун Е. В., Козелецкая И. К. Методы и средства защиты информации // The Scientific Heritage. 2020. № 51-1. С. 32–42.

2. Баринов С. В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. 2016. № 4. С. 97–105. DOI: 10.17803/1994-1471.2016.65.4.097-104

3. Богомолова Л. В. Информационная безопасность: что это такое в современных реалиях // Вестник науки и образования. 2023. № 1 (132)-1. С. 45–48.

4. Евтушенко И. И. Актуальные направления виктимологической профилактики дистанционных хищений // Виктимология. 2022. Т. 9, № 1. С. 90–98. DOI: 10.47475/2411-0590-2022-10909

5. Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. Т. 10, № 1. С. 78–88. DOI: 10.47475/2411-0590-2023-10108

6. Евтушенко И. И. Предупреждение виктимизации дистанционных хищений и сферы его воздействия // Виктимология. 2024. Т. 11, № 1 С. 43–56. DOI: 10.47475/2411-0590-2024-11-1-43-5

7. Курбанов Т. К., Карачаев А. Р., Пашаева Ф. Р., Гитинов Х. Х. Анализ методов защиты от несанкционированного доступа к личной информации // Образование и право. 2022. № 5. С. 325–329. DOI: 10.24412/2076-1503-2022-5-325-329

8. Лариков А. О. К вопросу информационной безопасности личности в информационном пространстве // Современное право. 2017. № 5. С. 28–32.

9. Никитин Е. В. Проблемы противодействия технологиям социальной инженерии как элементу преступной деятельности // Виктимология. 2023. Т. 10, № 4. С. 485–491. DOI: 10.47475/2411-0590-2023-10-4-485-491

10. Осипенко А. Л., Соловьев В. С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 681–691. DOI: 10.17150/2500-4255.2021.15(6).681-691

11. Панин О. Н., Сулейменова Р. Д. Угрозы безопасности цифрового профиля гражданина РФ // Молодой ученый. 2022. № 16 (411). С. 34–35.

12. Полякова Т. А., Чеботарева А. А. О новом «регуляторном ландшафте» в условиях цифровой трансформации системы права и экономики // Информационное право. 2020. № 2. С. 4–8.

13. Степанов О. А., Степанов М. М. Правовое регулирование генезиса цифровой личности // Правоприменение. 2022. Т. 6, № 3. С. 19–32. DOI: 10.52468/2542-1514.2022.6(3).19-32

14. Старостенко О. А. Виктимологические проблемы обеспечения безопасности личности в сети интернет // Вестник Сибирского юридического института МВД России. 2022. № 2 (47). С. 157–161.

15. Черецких А. В. Противодействие негативным методам социальной инженерии // Виктимология. 2023. Т. 10, № 4. С. 474–484. DOI: 10.47475/2411-0590-2023-10-4-474-484

ПРИЛОЖЕНИЕ А

Таблица А.1 — Виктимологическое обеспечение цифровой безопасности личности *

Как защитить себя сети Интернет?	
Повышайте безопасность личного профиля	Сложные пароли из 12 и более символов, включая специальные знаки, делают подбор путем перебора возможных комбинаций символов неэффективным. Двухфакторная аутентификация защищает аккаунт (профиль) даже в случае утечки
Устанавливайте только проверенное программное обеспечение (ПО)	Не используйте ПО из почтовых рассылок и с незнакомых сайтов. Это относится и к расширениям для браузера: вредоносные программы крадут цифровой ключ жертвы, с помощью которого преступник сможет беспрепятственно войти в аккаунт
Сохраняйте анонимность, когда это возможно	Желательно, чтобы личную страницу владельца нельзя было найти по имени и фамилии
Сохраняйте данные своей учетной записи втайне	Включая логин и номер телефона — по ним можно найти пароль в базах утечек
Зарегистрируйте несколько почтовых адресов	Например, отдельно для корпоративных сервисов и переписок. Не зная адрес электронной почты, преступники не смогут атаковать аккаунт, даже если у них есть имя и фамилия жертвы
Не переходите по ссылкам из подозрительных писем	Проверяйте доменное имя и адрес отправителя на ошибки. Добавьте важные сайты в избранное, чтобы не попасть на фишинговую страницу. Соблюдайте эти правила и уделяйте больше внимания данным о себе в открытых источниках, чтобы украсть личную информацию было сложнее
Используйте безопасные браузеры	Используйте только надежные и проверенные браузеры, не забывайте про брандмауэр и антивирусную программу. Также не переходите на социальную сеть по случайным ссылкам из интернета
Защитите доступ к своему Wi-Fi роутеру надежным паролем.	Обычно почти каждый человек, увидев, что нашлась бесплатная точка доступа, сразу подключаются к ней. А это может подвергнуть вас опасности. Будьте осторожны при использовании Wi-Fi
Как защитить себя в социальной сети?	
Используйте сложный пароль	Придумывайте как можно более длинный и сложный пароль. Добавляйте в свой пароль символы, иностранные буквы, цифры. Для каждой социальной сети придумывайте свой пароль — так безопасность ваша и ваших страниц будет повышена
Не указывайте личную информацию	В своем профиле как можно меньше пишите о себе, своих поездках, номерах телефонов и др.
Не выкладывайте фотографии с изображением нежелательных деталей и посторонних лиц	Перед тем как выложить фотографию, внимательно посмотрите на детали: на свой внешний вид, на окружающую местность, людей, находящихся рядом с вами и др.
Соблюдайте конфиденциальность	Установите параметры конфиденциальности. Незнакомые вам люди не должны видеть важные сведения о вас, которые могут быть расположены на странице
Как сохранить цифровую личность?	
Используйте банковскую карту с осторожностью	Кража банковских данных почти невозможна при оплате смартфоном или платежным стикером
Внимательно изучайте соглашения на обработку данных	Использование личной информации для обучения нейросетей встречается все чаще. Такие базы данных иногда утекают в сеть, в том числе из-за ошибки IT-специалистов

Продолжение таблицы А.1

Настройте уровень доступа приложений	Иногда в Google Play и AppStore попадают зараженные вирусом программы. Чтобы они не могли шпионить за владельцем и выполнять кражу информацию, ограничьте непроверенным приложениям доступ к камере, списку контактов и локальным данным в настройках системы. Уровень доступа можно задать в настройках iOS и Android
Блокируйте свои устройства, если работаете в публичных местах	Даже если вам нужно отойти на несколько минут
Ограничивайте распространение информации о себе	Не выкладывайте в соцсети фотографии личного характера, не указывайте домашний адрес, не описывайте подробности своей личной жизни, не сообщайте заранее о поездках, в особенности длительных. Не заполняйте в сети Интернет подробные анкеты для участия в сомнительных акциях, не оставляйте свои контактные данные непроверенным операторам
Убедитесь, что ваши имя, фотографии, личная информация не используется третьими лицами	Проверьте, не используются ли ваши фотографии на неизвестных вам ресурсах. Это можно сделать при помощи сервиса «Яндекс.Картинки». Если у вас редкие имя или фамилия, можно поискать данные о зарегистрированных на них аккаунтах
Сохраняйте конфиденциальность своей информации	Не размещайте в сети Интернет копии документов, рецептов, истории болезни. Удаляйте подобную информацию после отправки по электронной почте, в мессенджере или через файлообменник
Помните о кибербезопасности при использовании сети Интернет	Регулярно устанавливайте обновления ПО, используйте антивирус, раз в месяц удаляйте cookies, заходите только на сайты, использующие безопасное соединение https. Не пользуйтесь публичным Wi-Fi, регулярно меняйте пароли к своим аккаунтам
Как противостоять воздействию телефонных мошенников?	
Если номер абонента скрыт или неизвестен	— попросите абонента представиться еще раз; — уточните цель звонка абонента, если даже он уже об этом говорил; — убедитесь, что абонент дозвонился по адресу; — положите трубку и перезвоните в организацию, от имени которой к вам обратились
Если абонент сообщает, что звонок срочный/важный	— помните, что ни банки, ни полиция, ни другие организации не решают вопросы по телефону, особенно в срочном порядке; — если вам угрожают уголовной ответственностью за отказ сотрудничать — знайте, что телефонные угрозы не имеют юридической силы
Если входящий звонок через мессенджер	— государственные организации и банки не используют такой способ связи; — большинство руководителей организаций предпочитают личную беседу в кабинете
Если вам позвонили от имени вашего родственника или знакомого и просят перевести деньги	— свяжитесь с ним лично. Даже если он не подходит к телефону — это ещё не повод немедленно переводить деньги; — подождите, пока он перезвонит, или разыщите его через общих знакомых
Прежде чем выполнять любые указания, полученные по телефону	— возьмите паузу; — позвоните близким людям и обсудите с ними сложившуюся ситуацию

Окончание таблицы А.1

Дистанционные банковские операции	— не сообщайте по телефону данные о ваших банковских счетах, номера банковских карт, пин-коды, CVV/CVC/CVP-коды, коды из СМС и любые другие сведения для совершения банковского перевода
Определитель номера	— установите специальное приложение с определителем номера. Большинство номеров, используемых мошенниками находятся в базе, которая позволяет их распознать; — если вы уверены, что вам позвонил злоумышленник, сообщите номер мошенника в организацию, от имени которой он представился
«Голосовые помощники» и боты	— не видите диалог с «голосовым помощником», переданная вашим голосом информация может быть записана и в последующем использована в преступных целях; — спросите отчество у абонента, позвонившего вам. Если это «искусственный» абонент, то он не представится полным именем
Как понять, что звонок от мошенника	— позвонили вам, а не вы; — требуется принятие срочного решения вами; — разговор сводится к деньгам; — у вас просят коды (цифры), которые должны знать только вы; — просят назвать код (цифры) из отправленного вам СМС; — воздействуют на ваши эмоции и чувства

Таблица А.2 — Какие фразы произносят только мошенники? *

Фразы мошенников	Почему это неправда
«Давайте уточним ваши данные: назовите номер своего паспорта, номер банковской карты»	Настоящий сотрудник банка видит в информационной системе все данные клиента, сведения о его счетах и количестве денег, которые на них находятся
«Сколько у вас счетов в нашем банке?»	
«Уточните баланс каждого вашего счёта»	
«В каких ещё банках у вас есть счета?»	Банки работают автономно, сотрудник одного банка никак не может повлиять на то, что происходит в другом банке
«Нам надо составить заявку по факту мошеннических действий. Какую заявку будем составлять: обычную или экстренную?»	Если банк заподозрил, что с вашим счётом совершаются мошеннические действия, он заблокирует счёт без всякой заявки
«Вся информация о вашем лицевом счёте заблокирована»	Это не повод переживать! Вы можете спокойно пойти в офис банка и всё выяснить
«Вы не должны никому сообщать о данной операции, иначе будете нести уголовную ответственность» (здесь могут называться разные статьи Уголовного кодекса РФ)	Помните, что уголовную ответственность будет нести мошенник, который пытается выведать у вас информацию, а не вы

* Информация подготовлена на основе анализа способов защиты информации пользователей сети Интернет, клиентов банков и абонентов сотовой связи, представленной в открытом доступе на сайтах АО «Лаборатория Касперского» (URL: https://www.kaspersky.ru); ПАО «СберБанк» (URL: http://www.sberbank.ru); МВД РФ (URL: https://мвд.рф).

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует.

CONFLICT OF INTEREST
There is no conflict of interest.

Дата поступления статьи / Received: 25.04.2024.
Дата рецензирования статьи / Revised: 07.05.2024.
Дата принятия статьи к публикации / Accepted: 15.07.2024.