Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

Методические рекомендации
по подготовке и проведению Тематического урока на тему «Финансовая безопасность личности в сети Интернет»

Москва, 2023

Министерство образования и молодежной политики СО
28.02.2023
Вх.№ 4428

Аннотация

Методические рекомендации подготовлены в помощь педагогам образовательных организаций и ориентированы на оказание методической помощи педагогам основного общего, среднего (полного) общего и дополнительного образования по организации и проведению тематического урока, посвященного основам финансовой безопасности в сети Интернет. В методических рекомендациях предлагаются концептуальные, содержательные, методические и технологические подходы к проведению урока.

В Рекомендациях раскрывается комплекс вопросов, связанных с проведением данного мероприятия. Предлагаемые материалы носят рекомендательный характер, поэтому преподаватель может провести занятие, опираясь на данные разработки, исходя из собственного опыта, учитывая возрастные особенности, уровень подготовки обучающихся, а также традиции региона.

Пояснительная записка

Финансовое образование молодежи способствует принятию грамотных решений, минимизирует риски и тем самым способно повысить финансовую безопасность населения. Низкий уровень финансовой грамотности может привести не только к банкротству, но и к неграмотному планированию выхода на пенсию, уязвимости к финансовым мошенничествам, чрезмерным долгам и социальным проблемам, включая депрессию и прочие личные проблемы.

Цель – создание условий для формирования у обучающихся базовых представлений о финансовой грамотности и основных правилах финансовой безопасности личности в сети Интернет.

*Задачи***:**

- ✓ сформировать убежденность обучающихся в том, что финансовая грамотность и финансовая безопасность – личная (семейная) и государственная, – основа финансового благополучия;
- ✓ заложить у обучающихся установки грамотного финансового поведения в сети Интернет, закрепить базовые финансовые понятия, отработать алгоритм решения сложных жизненных ситуаций, связанных с опасностью стать жертвой утечки персональных, в том числе биометрических, данных;
- ✓ сформировать у обучающихся общее представление о финансовых рисках в современной экономической ситуации; понимание системной взаимосвязи личной финансовой безопасности и финансовой безопасности государства; понимание опасности для государства и граждан преступлений в сфере финансов.

На фоне цифровизации всех сфер нашей жизни молодежь становится активным пользователем финансовых услуг в Интернете. Так, каждый третий подросток использует безналичный способ оплаты, а каждый второй – совершает покупки с помощью смартфона.

Сравнительно высокий уровень цифровой грамотности[1] и наличие смартфона позволяет подросткам использовать мобильный и интернет-банк (56% и 38% соответственно).

Несмотря на то, что наличные остаются наиболее распространенным способом оплаты у подростков (42%), большая их доля совершает покупки безналично (32%). Почти половина подростков (43%) бесконтактно расплачивается с помощью смартфона.

Согласно статистическим данным Национального агентства финансовых исследований (НАФИ)[2], в России только 10% населения демонстрируют стабильно высокий уровень финансовой грамотности, причем наиболее финансово грамотные люди в России – это мужчины и женщины в возрасте 40-49 лет, имеющие высшее образование, а также жители крупных городов.

Каждый второй представитель молодежи (53%) считает, что ему не хватает знаний о финансовой безопасности: по мнению 48% опрошенных, некоторые знания в этой сфере у них есть, но их недостаточно для того, чтобы защититься от мошенничества, а 5% заявляют, что знаний о безопасном обращении с финансами у них нет вообще. Чаще не уверены в своих знаниях подростки в возрасте от 14 до 17 лет (53%).

Среди российской молодежи популярен ряд неверных установок с точки зрения финансовой безопасности[3].

В первую очередь, это ошибочное восприятие надежности криптовалюты как инструмента инвестирования: 65% молодых россиян не осознают высокие риски цифровой валюты и считают, что вложения в нее являются одним из надежных способов уберечь деньги от инфляции. Такая позиция в большей степени характерна для молодых жителей крупных городов (49%) и опрошенных от 18 до 24 лет (46%).

Почти две трети представителей молодежи ошибочно убеждены, что существует много простых способов преумножения капитала (с этим согласны 60% опрошенных). Непонимание соотношения риска и доходности финансовых инструментов тем самым создает предпосылки для массового вовлечения молодых людей в высокодоходные и часто нелегальные, сопровождающиеся высокими рисками, инвестиционные схемы.

Молодежь также пренебрегает защитой персональных данных при совершении онлайн-платежей. Более половины молодых россиян (59%) не уделяют должного внимания сохранности своих персональных данных, совершая покупки в интернете. Чаще других об этом заявляют представители зрелой молодежи (57% среди опрошенных в возрасте от 25 до 35 лет).

---

[1] Уровень цифровой грамотности подростков составляет 73 п.п. из 100, для сравнения — индекс взрослых равен 52 п.п./

[2] Данные с портала «Мои финансы» // URL: https://xn--80apaohbc3aw9e.xn--p1ai/article/finansovaya-gramotnost-rossiyan-vyrosla-za-poslednie-4-goda/ (дата обращения: 19.01.2023).

[3] Репрезентативный опрос молодежи проведен в июне 2022 г. с помощью онлайн-панели Тет-о-Твет-М. Опрошены 1000 человек в возрасте от 14 до 35 лет. // URL: https://nafi.ru/analytics/kazhdyy-vtoroy-predstavitel-molodezhi-schitaet-chto-emu-nedostatochno-znaniy-o-finansovoy-bezopasnos/ (дата обращения: 19.01.2023).

В современном мире биометрические данные становятся основным средством идентификации личности при совершении финансовых операций в сети Интернет: по результатам исследования платежной системы Visa, банки и платежные системы опередили социальные сети, производителей мобильных телефонов и сотовых операторов по уровню доверия со стороны россиян – 48% респондентов доверяют им хранение своих биометрических данных.

Самое большое предпочтение из биометрии респонденты отдают отпечатку пальца (92% респондентов), лицо в идентификации используют 17% опрошенных, голос — 12%. При этом паролям и пин-кодам россияне симпатизируют меньше. Тем не менее 51% опрошенных имеют несколько паролей к своим аккаунтам. При этом каждый десятый пользуется лишь одним паролем для входа во все аккаунты. Как отмечает Visa, именно трудности с запоминанием подталкивают россиян к использованию одного и того же пароля для разных аккаунтов, тем самым повышая риск их взлома мошенниками. Идентификация по биометрии избавляет от запоминания множества паролей и пин-кодов — и это главное преимущество, считают 47% опрошенных.

Каждый человек может столкнуться с мошенничеством при потреблении финансовых услуг, утечкой персональных данных при совершении онлайн-покупок. Большинство подобных инцидентов можно избежать, применяя правила и меры предосторожности в этой области, объединяющиеся под общим названием «финансовая безопасность».

В последнее время финансовые потери случаются очень часто на всех уровнях, затрагивая и макроэкономический (общегосударственный, национальный) уровень, и уровень отдельных граждан. Финансовая безопасность личности зависит как от уровня финансовой и, шире, экономической безопасности государства, так и от финансовых решений, принимаемых самим гражданином, то есть уровня его осведомлённости в вопросах финансовой грамотности в целом, и финансовой безопасности, в частности.

Раскрытие основной темы урока направлено на формирование основ финансовой культуры обучающихся, воспитание понимания ими важности приобретения базовых знаний и навыков обеспечения личной финансовой безопасности и ее взаимосвязи с финансовой безопасностью государства.

Основой урока станут ответы на ряд вопросов: «Как защитить свои права как потребителя финансовых услуг? Как обезопасить свои персональные данные от утечки? Как обезопасить себя от злоумышленников в социальных сетях и онлайн-играх?».

В рамках подготовки к уроку можно задействовать информационные видеоролики, комиксы и брошюры, посвященные финансовой безопасности.

Обучающимся можно предложить решить ситуационные задания, проанализировать статистические данные и теоретический материал на тему финансовой безопасности личности в сети Интернет, порассуждать на

предложенную педагогом тему, высказать свое мнение и поделиться собственным опытом в отношении ситуаций, когда у человека может возникнуть потребность во владении тем или иным правилом финансовой безопасности.

В ходе подготовки к проведению урока учителя могут обратиться к материалам медиатеки Международного учебно-методического центра финансового мониторинга (https://mumcfm.ru/mediateka), образовательно-просветительского сервиса Научно-исследовательского финансового института Министерства финансов Российской Федерации (моифинансы.рф).

Особенности организации учебной деятельности

Важным условием достижения педагогических задач является организация урока таким образом, чтобы фронтальная, групповая и индивидуальная работа взаимно дополняли друг друга. При подготовке и проведении занятия необходимо учитывать возрастные и образовательные возможности обучающихся. Возможно изменение объема учебного времени, отводимого на тот или иной раздел урока в зависимости от возможностей и потребностей обучающихся.

Основные тезисы урока

Современное общество стремительно развивается во всех сферах, не исключением становятся и финансы, которые сегодня вбирают в себя все последние достижения научного прогресса. В такой ситуации главное не просто научить человека действовать по алгоритму (что тоже очень важно при решении многих финансовых задач), а сформировать компетенцию ориентироваться в финансовом пространстве, оценивать различные альтернативы решения финансовых проблем и принимать оптимальное решение в конкретных жизненных обстоятельствах.

Результаты исследования Международного учебно-методического центра финансового мониторинга (МУМЦФМ)[4] показали, что молодежь проявляет наибольший интерес к тем аспектам финансовой безопасности, которые связаны с защитой их личных прав в финансовой сфере (78%), информационной безопасностью личности в финансовой сфере (67%) и обеспечением безопасности биометрических персональных данных (73%).

В нашем обществе на современном, «информационном» этапе его развития, информация является наиболее значимым ресурсом, а информационное поле – основным местом обитания современного человека.

В основе всех доступных нам сервисов, услуг, с помощью которых мы в том числе управляем нашими финансовым активами и осуществляем

[4] Репрезентативный опрос молодежи проведен в партнерстве с МУМЦФМ в сентябре 2022 г. Опрошены 1000 человек в возрасте от 14 до 35 лет. / URL: https://nafi.ru/analytics/finansovaya-bezopasnost-chemu-i-kak-obuchat-molodezh-/ (дата обращения: 9.01.2023).

финансовые операции, лежат различные виды *данных*, среди которых непосредственное отношение к нам имеют *персональные данные*.

В сети Интернет хранится бесчисленное множество наших персональных данных, формирующих т.н. «цифровой профиль» человека – набор всех следов существования, которые он оставляет в цифровом мире. С течением времени таких следов становится все больше: внедряются новые гаджеты (например, умные часы для мониторинга состояния здоровья), технологии отслеживания перемещений и общения, цифровая идентификация личности.

Добавляя новые данные к уже привычным фотографиям, паролям, истории поиска в Интернет-браузере, сфере интересов, мы получаем полный набор индивидуальных черт и особенностей человека, только оцифрованный. Анализ большого объема данных о человеке (или цифровой анализ личности) позволяет судить о его интеллектуальном уровне, компетенциях, возможностях, перспективах.

Несмотря на то, что цифровые технологии упрощают нашу жизнь во многих аспектах, они же порождают и множество угроз. Неконтролируемый сбор информации о человеке порождает для него ряд опасностей – от безобидных, но назойливых спам-звонков до манипулирования мнением, сознанием, кражи его «цифровой личности» и денежных средств.

Что такое «персональные данные»?

Персональные данные – любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных), то есть это любая информация, которая прямо или косвенно указывает на вас, или как-то связана с вами.

Существует несколько *видов персональных данных*:

а) общие – фамилия, имя, отчество, паспортные данные, дата и место рождения, адреса регистрации и места проживания;

б) специальные категории персональных данных, к которым относятся национальность, политические, религиозные или философские взгляды и убеждения, сведения о состоянии здоровья, интимной жизни, судимости;

в) общедоступные персональные данные, разрешенные лицом для распространения (информация, которую предоставляем неограниченному кругу лиц через социальные сети, например);

в) биометрические персональные данные – отпечатки пальцев, рисунок радужной оболочки глаза, рисунок вен ладони, код ДНК, слепок голоса;

г) обезличенные – данные, по которым невозможно установить человека, не имея дополнительных данных (таблица со значениями идентификаторов).

РАЗДЕЛ I. Цифровой профиль личности и биометрические персональные данные

Алгоритмы сегодня знают о человеке гораздо больше, чем его собственные родители, имея в своем распоряжении не просто информацию о

чем-то конкретном – целый пласт данных, который открывает возможность создать конкретную личность в цифровом мире, аналог живого человека.

Понятие цифровой личности прочно входит в обиход, и мы уже отделяем его от понятия «профиля» в социальных сетях. Если первое определение больше используется в научном мире, в разработках, то со вторым уже имеют дело практически все. В этом ключе и следует рассматривать вопросы финансовой безопасности цифровой личности.

Как происходит похищение цифровой личности?

После перехода многих сфер деятельности человека в Интернет цифровая личность также приобрела цену. Она стала товаром со своими характеристиками, ценностью и стоимостью. И речь идет не просто о завладении паролем или правом доступа.

В основе всего современного маркетинга лежит цифровой анализ личности. За сведения о предпочтениях человека, его образе жизни и потребностях готовы платить. Причем чем больше компании готовы вкладывать, тем больший объем данных получают они в свое распоряжение. Благодаря этому работают «умные ленты», точечные показы рекламы, отслеживание потоков людей при показах рекламы – этим уже никого не удивишь, но мы также не до конца знаем, насколько далеко простирается данный анализ.

Даже взрослый человек, не говоря о подростках, не в состоянии дать свое осознанное согласие на то, чего не до конца понимает, в том время как цифровая личность может легко стать объектом неправомерных действий. Такие явления, как похищение цифровой личности, уже присутствуют в современной реальности. Если компания работает с управлением финансами граждан и бизнеса, большое количество людей заботят вопросы о том, что она делает с информацией об их финансовых активах, целях инвестирования, готовности к рискам и т.д.

Другой пример: в начале 2019 года стало известно о торговой площадке Genesis, через которую продавали более 60 тысяч украденных цифровых личностей, а также о специальном браузере со встроенным генератором цифрового следа человека.

Какую информацию крадут?

Кража цифровой личности – *фото, видео с ваших страниц в социальных сетях, аккаунтов и профилей, паспортных данных и копий документов, селфи с документами, фото банковских карт* – может быть совершена с разными целями: от банальной продажи информации до шантажа, использования в мошеннических схемах. Самый простой пример — использование номеров телефонов, имен, сведений из жизни и голоса для обмана и мошенничества.

Зачем крадут цифровую личность?

Доступ к чужому аккаунту открывает широкие возможности. Можно читать переписку и вести её от имени владельца, можно следить за ним, искать конфиденциальную информацию, публиковать от его лица контент, просить перевести денег, распространять спам, использовать для раскрутки рекламных

групп. Все это – угрозы, которые несет в себя утеря персональных данных, составляющих цифровую личность конкретного человека.

1. *Мошенничество*. Под видом знакомых нам людей мошенники, создавая фейковые аккаунты, вынуждают, убеждают нас переходить на незнакомые сайты, позволяющие им получить доступ к нашим деньгам.

2. *Получение бонусов и услуг по постоплате*. Некоторые из нас сталкивались с рекламой букмекерских компаний, форекс-сайтов, онлайн покер-румов и других сайтов, предлагающих новым клиентам деньги на счёт, на которые вы можете воспользоваться услугами. Украденные данные будут использованы злоумышленником для создания аккаунта с целью получения бонусов. Как правило, это достаточно безобидно для жертвы, разве что вы не сможете воспользоваться рекламным предложением в будущем. Куда менее радужными могут быть последствия приобретения на украденные данные услуг по постоплате, когда злоумышленник регистрирует на ваши данные аккаунт, использует услуги, а в конце вместо их оплаты просто исчезает. В этом случае от вашего имени совершается полноценное мошенничество.

3. *Регистрация аккаунтов*. Фотографии людей используются при создании аккаунтов для спама в социальных сетях, это увеличивает частоту успешных атак. Зачастую злоумышленники не утруждают себя менять данные и берут реальные данные жертвы, включая имя и фамилию. В сети можно найти предложения о продаже аккаунтов в различных социальных сетях и иных сайтах. Для регистрации подобных аккаунтов злоумышленники также используют краденные данные, реже подобные аккаунты собираются в результате фишинга или утечек данных.

4. *Получение займа*. Сегодня, в условиях большой конкуренции, компании, занимающиеся онлайн-займами, повсеместно понижают планку требований к заемщикам, упрощая процедуру получения небольшой суммы. Подобные риски окупают высокие проценты по займам, которые иногда доходят до тысячи процентов в год, и большие штрафы за любую просрочку. Минимизация проверок и предоставляемых данных превратила онлайн-займы в лакомый кусок для мошенников, берущих займы на чужие данные. В некоторых случаях мошенникам хватит электронных копий двух документов жертвы, например, паспорта и прав. Можно для их получения создать объявление о работе и просить у потенциальных соискателей после «принятия» на работу копии документов. Мошенники знают много способов получить копии документов и взять на них займ. Бывают и более изощренные схемы мошенничества с получением займов без ведома владельца. На одном из русскоязычных андеграунд форумов как-то появилось предложение о продаже авиабилетов за 50% от их реальной стоимости. Предлагавший услугу владелец сервиса заверял, что никакого мошенничества нет, авиабилеты не покупаются на краденные средства. Первое время посетители форума относились с недоверием к заманчивому предложению, затем положительные отзывы начали привлекать все больше и больше клиентов. Клиенты отправляли злоумышленнику все данные, включая ксерокопии документов.

Ни у одного из клиентов не возникло проблем с полетом. Проблемы возникли позже, когда банк, в котором эти билеты оформлялись в кредит, начал требовать вернуть сумму за авиабилеты, проценты и внушительные пенни за просрочки. В итоге жертвы заплатили по 200-300 процентов от реальной стоимости приобретённых билетов.

5. *Месть и нанесение вреда репутации*. В сети можно найти немало историй как недоброжелатели, желая отомстить кому-либо, выставляли его фотографию и анкету на различных сомнительных сайтах. Главная проблема в том, что даже если сайт удалит фотографию и профиль жертвы, к этому времени другие сайты, копирующие данные, разместят у себя ее профиль, фотография попадёт в поисковую выдачу по картинкам. Удалить данные со всех сайтов и поисковых систем часто становится практически неразрешимой задачей, особенно если у жертвы нет на это достаточных средств. Если вы человек, зависимый от репутации, недоброжелатели могут попытаться испортить вам ее. Например, размещать от вашего имени отзывы на товары для взрослых. Все, кто в дальнейшем будут искать информацию о вас, будь то работодатели или потенциальные партнеры, наткнутся на подобные, не красящие вас, отзывы. Любой пользователь может стать жертвой утечки данных, когда учётные записи оказываются в сети из-за технической уязвимости или действий злоумышленников. Проверить, не попали ли эти данные в открытую базу, можно с помощью *специального сайта*, который накапливает информацию об утечках аккаунтов.

Скептики говорят, что злоумышленники смогут получить личную информацию в любом случае, если это будет необходимо, но лучше максимально усложнить им путь к вашим данным.

Что делать в случае утечки?

В случае, если ваши персональные данные попали в сеть и оказались выложены на одном или нескольких сайтах, эффективными могут быть следующие меры.

1. *Обращение к владельцу сайта*. Самый простой и часто самый эффективный метод, если ваши персональные данные утекли и выложены на одном или нескольких сайтах. Вежливо, без угроз, попросите владельца сайта вам помочь. Если вежливое обращение не поможет, предупредите, что вы будете вынуждены обратиться в суд и к регулирующему органу с одной-единственной целью – защитить ваши персональные данные.

2. *Обращение в регулирующий орган*. В России это Роскомнадзор. Напишите обращение, в котором сообщите, что указанный сайт распространяет персональные данные без вашего разрешения, нарушая законы Российской Федерации. Обязательно укажите ссылку на выложенные данные. Максимум, на что способен регулирующий орган – оштрафовать владельца, если он установлен и находится в одной правовой юрисдикции с самим органом, либо заблокировать его на территории страны размещения регулирующего органа. Для многих владельцев сайтов блокировка на

территории той или иной страны – серьезная потеря аудитории, и они незамедлительно удаляют контент, ставший причиной блокировки.

3. *Жалоба хостинг-провайдеру и регистратору.* Хостинг-провайдер – организация, предоставляющая сайту сервер для размещения, регистратор – организация, где владелец сайта зарегистрировал доменное имя. Вам надо зайти на сайты регистратора и хостинг-провайдера и найти там контакты для жалоб, обычно они содержат слово «abuse». Даже если такого контакта не обнаружится, обратитесь по любым доступным контактам.

4. *Обращение к борцам с мошенниками*. Если сайт является мошенническим (например, торгует документами, или ваши персональные данные выложены там с целью вымогательства), стоит предупредить об этом организации, занимающиеся борьбой с подобными сайтами или составляющие базы опасных сайтов.

5. *Обращение в суд.* Если обращение к владельцу сайта, хостинг-провайдеру и регистратору не принесли положительного результата, вам необходимо найти адвоката и задуматься об обращении в суд. Суд может принять решение, согласно которому страница с персональными данными будет заблокирована на территории вашей страны, а также обязать поисковые системы удалить из выдачи ваши персональные данные. Однако возможности суда сильно зависят от законодательства вашей страны, стоит проконсультироваться по данному вопросу с юристом. Эффективность метода также завязана на возможностях суда, в России это один из самых эффективных методов. Нередко владельцы сайтов, чтобы с них сняли ограничения, удаляют заблокированный решением суда контент.

6. *Обращение в правоохранительные органы*. В России, как и во многих других странах, распространение или продажа персональных данных является уголовным преступлением. Стоит уведомить правоохранительные органы о сайте, нарушающем закон. К счастью, сегодня для этого необязательно идти в ближайший участок, отстаивать очередь и писать заявление, все это можно сделать онлайн.

7. *Изменение данных документов.* Если вы опасаетесь, что выложенную ксерокопию вашего документа могут использовать в мошеннических целях, например, оформить заем, разумным шагом будет обратиться в правоохранительные органы и сменить номер документа. Такая возможность доступна не во всех странах, вам лучше обратиться к юристу для уточнения деталей.

Как предотвратить кражу цифровой личности?

Чтобы обезопасить свои данные, необходимо соблюдать элементарные *правила цифровой гигиены*:

- ✓ не делиться о себе большим количеством информации в сети;
- ✓ создавать сложные и разные пароли, ещё лучше – пользоваться менеджером паролей для их создания и хранения;
- ✓ везде, где это возможно, настроить двухфакторную аутентификацию для входа в аккаунт;

✓ не хранить конфиденциальные документы и приватные фотографии в открытом виде на устройствах – смартфонах, планшетах, ПК;

✓ поставить защитное решение на все устройства и регулярно обновлять его; важно, чтобы это был не просто антивирус, а комплексное решение для защиты от фишинга, онлайн-мошенничества, веб-слежки, с функцией безопасных платежей;

✓ устанавливать приложения только из официальных магазинов и внимательно проверять, какие разрешения вы даёте установленным приложениям;

✓ не переходить по сомнительным ссылкам, не воспринимать заманчивое предложение как призыв к действию;

✓ с осторожностью относиться к звонкам с незнакомых номеров, к сообщениям от неизвестных отправителей, к любым просьбам перевести денег;

✓ использовать для передачи почтовые сервисы с возможностью удалить данные у получателя: подобный функционал есть у Gmail;

✓ обязательно удалять из электронного почтового ящика и мессенджеров письма, содержащие персональные данные на случай взлома вашего почтового ящика, особенно если вы пересылали куда-то сканы своих документов;

✓ попросить адресата уважительно отнестись к вашим персональным данным: отправляя письмо с документами по почте или в мессенджере, сопроводите его просьбой уважительно отнестись к вашим персональным данным

✓ не называть ксерокопии документов ключевыми словами: в некоторых социальных сетях, например, ВКонтакте, документы, загружаемые пользователями, попадают в публичный доступ, поэтому, любым ценным документам, как бы они ни передавались и хранились, лучше давать нейтральные заголовки, например, «pic15» или «image1988»;

✓ не использовать социальные сети для авторизации на сайтах: в обмен на это вы предоставляете сайту доступ к своим персональным данным, которые он собирает, иногда продает, иногда у него их воруют злоумышленники;

✓ удалять все неиспользуемые аккаунты: утечки с сайтов – один из самых распространенных путей кражи личности;

✓ при пересылке копий своих документов, указывать на них дату и адресата (либо сайт, куда отправляете данные) с помощью водяного знака или приложенной к фото документов бумажкой с написанными на ней данными адресата: даже если копия попадет в руки злоумышленников, они не смогут использовать ее на других сайтах и, скорее всего, удалят как бракованный товар.

Соблюдение этих правил позволит хотя бы затруднить доступ мошенникам к важной части сведений о вас как о человеке, поможет снизить риск потери денег, репутации, времени. Если сам пользователь уделит больше

внимания тем данным, которые он предоставляет о себе сознательно или машинально, похищение цифровой личности не будет столь элементарным.

Защита биометрических персональных данных

Подразделение IBM Security корпорации IBM выпустило в начале 2018 года глобальное исследование, посвященное мнению потребителей о цифровой идентификации и аутентификации. В исследовании IBM Security «Будущее систем идентификации» приняли участие около 4 тыс. совершеннолетних жителей США, стран Азиатско-Тихоокеанского региона (АТР) и Европы. Согласно его результатам, при входе в приложения и устройства пользователям более важен уровень безопасности, а не удобство использования. Более того, по данным исследования, молодежь уделяет меньше значения безопасности традиционной идентификации с помощью пароля. Для входа в систему они предпочитают использовать биометрию, многофакторную аутентификацию и диспетчер паролей, чтобы повысить личный уровень информационной защиты. Биометрия становится «мейнстримом»: 67% респондентов успешно используют биометрическую аутентификацию, в то время как 87% опрошенных заявили, что будут применять эту технологию и в будущем.

Результаты опросов показали, что подростки и молодежь оставляют пароли в прошлом: 75% опрошенных уже используют биометрическую идентификацию. При этом меньше половины из них используют сложные пароли для входа в систему, а 41% – повторно используют свои пароли. Люди старшего поколения больше внимания уделяют созданию надежного пароля, но менее склонны к использованию биометрии и многофакторной аутентификации.

На фоне стремительного распространения использования биометрии как способа распознавания (идентификации) человека для различных целей – например, для идентификации в пропускных системах офисов, в компьютерных системах, смартфонах, платежных сервисах; идентификации пользователей финансовых услуг – особенно актуальным становится вопрос обеспечения защиты данного вида персональных данных.

Биометрические данные уникальны для каждого человека, они не повторяются и не изменяются в течение жизни.

К биометрическим персональным данным относятся: отпечатки пальцев; рисунок вен ладони; рисунок радужной оболочки глаз; код ДНК; образ лица; слепок голоса; рост; вес; особенности строения тела; изображения человека (фотографии, видеозаписи); иные физиологические и биологические характеристики человека (например, походка).

Угрозы неправомерного использования биометрических персональных данных и способы защиты от них

1) Дипфейки – реалистичная подмена фото, аудио и видеоматериалов, созданная с помощью нейросетей. Используя компьютерные алгоритмы, можно «оживить» фотографии, заменять лица на видео и даже синтезировать голос человека.

Дипфейки может создавать практически каждый в силу доступности обучения и количества программ для работы с этой технологией. Такой низкий порог входа двигает технологию вперед, но также увеличивает количество инструментов у мошенников для обмана пользователей и кражи их персональных данных.

Дипфейки могут быть использованы для манипулирования нашим сознание: например, с помощью этой технологии могут быть созданы провокационные видео с резкими заявлениями политиков либо видеообращение известного блогера, которые либо вызывают большой резонанс в обществе, либо призывают зарегистрироваться на каком-либо сайте, чтобы поучаствовать в розыгрыше призов. Особенно опасно, если вместе с такими видео распространяется ссылка на фишинговый сайт. Но наиболее распространенным способом использования дипфейков остается вымогательство – притворяясь друзьями, родственниками или начальством мошенники могут получать персональные данные человека, используя голосовые или видеосообщения, как подтверждение своей личности.

2) Программы распознавания лиц – нейросети, которые анализируют уникальные черты человеческого лица и сравнивают их с другими фотографиями в различных базах.

Наверняка каждый из нас хотя бы раз пользовался поиском по картинке в браузере. С помощью алгоритмов, позволяющих собирать ключевую информацию о человеке по его фото, можно найти его аккаунты в социальных сетях и использовать его персональные данные. Для такого поиска достаточно загрузить фотографию человека, и программа выдаст информацию о нем из открытых источников. Благодаря такому «портфолио» на жертву мошенники с легкостью составят подходящую схему обмана, чтобы вытянуть еще больше персональных данных, а затем и денег.

Как защититься от мошенников, использующих чужие биометрические данные?

- ✓ Не стоит пользоваться программами распознавания лиц, поскольку таким образом ваши данные попадут в их базу, и вы станете гораздо более уязвимой целью для мошенников.
- ✓ Закрывайте свои профили в социальных сетях – так программы не смогут найти ваши фото при анализе.
- ✓ В социальных сетях добавляйте в «друзья» только проверенных людей, которых вы знаете лично
- ✓ Мошенники чаще всего используют открытые ресурсы для создания дипфейков. Если ограничить доступ к вашим аккаунтам в социальных сетях и мессенджерах (настроить приватность), то у них будет меньше шансов создать с вашей личностью что-то правдоподобное.
- ✓ Публикуйте только необходимую информацию и убедитесь, что на страницах ваших друзей и знакомых минимум ваших персональных данных, либо же их нет совсем.

- ✓ Проверьте данные о розыгрышах, конкурсах или мероприятиях на официальном сайте компании или в действительном аккаунте знаменитости, от лица которых проводится акция. Не стоит переходить по неизвестным ссылкам даже если на сопровождающем публикацию фото реальное изображение известного человека.
- ✓ Будьте бдительны – всегда находите первоисточник или анализируйте материал, прежде чем совершать какие-либо действия. Мошенники постараются создать стрессовые условия, чтобы вынудить вас принять решение незамедлительно. Не поддавайтесь таким уловкам, даже если на первый взгляд все выглядит правдивым.

РАЗДЕЛ II. Финансовая безопасность в социальных сетях и онлайн играх

Социальные сети стали неотъемлемой частью нашей повседневной жизни. Так, в 2019 году Всероссийский центр изучения общественного мнения (ВЦИОМ) опубликовал исследование, по результатам которого почти 90% российских подростков пользуются социальными сетями каждый день или «практически ежедневно». На страничках в социальных сетях мы размещаем много информации о себе – это, пожалуй, самое большое хранилище информации, которое находится в открытом доступе и до которой мошенникам добраться проще всего.

Это не означает, что для того, чтобы себя обезопасить и не стать жертвой мошенников, нужно отказаться от использования социальных сетей. Просто важно знать какие угрозы существуют и правила, которые помогут защитить себя.

Наиболее опасной угрозой мошенничества в социальных сетях является вовлечение пользователей в финансирование террористической и экстремистской деятельности с помощью обмана. *Финансирование терроризма* – предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения любого из преступлений террористической направленности, или для финансирования или иного материального обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества, созданных или создаваемых для совершения таких преступлений.

Террористические группы активно используют Интернет, в частности, социальные сети для пополнения своих финансовых ресурсов. Глобальные сети сбора денег крупных террористических организаций построены так же, как и сети неправительственных организаций, благотворительных фондов и других финансовых учреждений. На сайтах, форумах и в чатах встречаются прямые просьбы помочь «делу джихада» посредством перечисления

денежных средств либо обманные призывы перечислить денежные средства в поддельные благотворительные фонды для помощи попавшим в беду.

Фишинг в социальных сетях

Этот вид мошенничества имеет множество форм и подразумевает использование популярных социальных сетей для того, чтобы завладеть чужой учетной записью, украсть конфиденциальные данные жертв, или заманить их на фейковые сайты с целью обогащения. Мошенники могут создавать фейковые (поддельные) аккаунты, выдавая себя за кого-то из знакомых потенциальной жертвы, чтобы заманить ее в свою ловушку, или они могут даже выдавать себя за аккаунт службы обслуживания клиентов известной компании, чтобы охотиться на жертв, которые обращаются в эту компанию за поддержкой.

Также через социальные сети мошенники могут предложить купить различный товар с большими скидками и вы, переходя по предложенным в аккаунте ссылкам, попадаете в ловушку: не получаете товар и теряете деньги.

Чем опасен фишинг в социальных сетях?

Взломав ваш аккаунт и получив доступ к вашим перепискам, отправленным и полученным файлам, базе подписчиков, мошенники получат широкие возможности для различных видов шантажа, публикации провокационной информации и социальной инженерии: прикрываясь вашей личностью, мошенник может связаться с каждым из списка контактов – так может быть запущена цепная реакция мошеннических активностей. Нередко такие рассылки происходят в ночное время, так как мошенники часто работают из других стран (это усложняет процесс поиска мошенника правоохранительными органами).

Наиболее опасные *виды фишинга:*

1) Сообщения с просьбой денежного займа, голосования в конкурсе, ссылкой на «смешное видео» от кого-то из ваших друзей. При переходе на страницу голосования или для просмотра «смешного видео» вам предлагается ввести логин и пароль на странице, похожей на главную страницу социальной сети, после чего аккаунт оказывается взломанным.

2) Интернет-магазины, кинотеатры, службы доставки и прочее. Здесь целью становятся данные, позволяющие получить доступ к привязанным банковским картам. Согласно исследованию Group-IB, в 2020 году такие сервисы стали целью в 30,7% случаев мошеннических атак[5]. В зоне риска находятся и те, кто вводит платежные данные в онлайн-магазинах: ошибившись с окном ввода, не проверив адрес в строке браузера, вы рискуете отправить деньги мошеннику. Тем более, что существуют сервисы, имитирующие ошибку транзакции с целью ее повторения, например, чтобы провести транзакцию два раза подряд.

3) Игра на чувствах и эмоциях через публикацию на страницах социальных сетей очень эмоциональных историй о детях или животных, нуждающихся в помощи, с подкреплением поста фотографиями, документами

[5] Официальный сайт Group-IB https://www.group-ib.ru/resources/threat-research.html

и сообщением «максимальный репост». Главное – создать конверсию поста и его распространение от одного человека по цепочке его друзей и контактов. Конечно же деньги от такой «псевдоблаготворительности» идут мошенникам!

4) Игра на любопытстве. Вы можете получать заманчивые предложения в личных сообщениях, либо в ленте. В любом случае вас попросят перейти по какой-либо ссылке и ввести личные данные или данные банковской карты.

Основные правила защиты от фишинга в социальных сетях:

✓ Как только вы узнали, что данные утекли или потенциально могли быть украдены мошенниками, как можно быстрее меняйте пароли от социальных сетей, почты, платежных сервисов. А лучше менять пароли раз в три месяца!

✓ Никогда не используйте одинаковые пароли. Правило «1 пароль, 1 сервис» поможет прервать запущенную фишинг-цепочку по проверке соответствия ваших логина и пароля другим популярным сервисам. Сегодня мошенники используют автоматические сервисы, позволяющие очень быстро проверить, куда еще могут подойти ваши данные.

✓ Будьте внимательны. Избегайте спешки в момент ввода логина, пароля и платежных данных. Проверьте адресную строку, присмотритесь к элементам дизайна. Если что-то смущает, вводить данные не следует!

✓ Используйте двухфакторную аутентификацию. Если ваши логин и пароль окажутся в руках взломщиков, для входа потребуется ввести полученный на телефон код, или использовать дополнительное приложение.

✓ Не доверяйте сомнительным предложениям и ссылкам. Ссылка, скрытая сервисом коротких URL, подобным bit.ly, может привести к мошенникам. Если стилистика сообщений или манера общения вашего друга в чате изменилась – возможно, это повод ему позвонить и удостовериться, что вам пишет именно он.

Фейковые аккаунты: чем они опасны и как их распознать?

Поддельный профиль в социальной сети – один из способов выманить личные данные и деньги пользователей.

Создаваться фейковые странички могут по разным причинам.

1. Самая безобидная из них – когда человек по каким-либо личным причинам не хочет афишировать свое присутствие в социальной сети. Фамилия и имя, как правило выдуманные. Вместо аватарки цветы или котики, друзей мало или вовсе нет.

2. *Сайты магазинов*, которые предлагают популярные или дефицитные товары по очень низким ценам, и обычно просят перевести полную стоимость прежде, чем отправят товар. И даже если вы в последний момент передумали платить вперед, то наверняка отправили мошенникам личные данные: кому доставлять и куда. Они будут рады и этому – а уж как использовать вашу личную информацию, непременно придумают.

Что делать:

✓ проверяйте информацию об акциях на официальных сайтах магазинов;

- ✓ помните, что крупные магазины вряд ли будут рассылать новость о розыгрыше через социальные сети, для этого они скорее используют СМС или электронную почту;
- ✓ стоит насторожиться, если вас просят рассказать об акции большому количеству знакомых, – это типичный способ мошенников распространить свои ссылки.

3. *Взломанный аккаунт реального человека*. С таких профилей могут приходить сообщения со спамом (чаще всего запрещенная к распространению информация или вредоносные ссылки) либо агрессивные и оскорбительные письма, призванные спровоцировать вас поинтересоваться личностью «хейтера» и, возможно перейти по ссылке (часто единственной), размещенной в его профиле. Но чаще мошенники отправляют всем друзьям письма с просьбой о финансовой помощи или просто выручить деньгами до завтра. Если вам вдруг будут приходить письма от друзей с такими мольбами, будьте уверены – это, скорее всего, обман. Для того, чтобы не быть обманутым, лучше поинтересоваться у друга лично, позвонив ему.

Что делать:

- ✓ не реагируйте на негативные комментарии: просто заблокируйте пользователя и удалите сообщение;
- ✓ не переходите куда-либо со страниц незнакомых вам пользователей, особенно если единственная доступная опция на них – это кликнуть по предложенной ссылке;
- ✓ внимательно проверяйте все страницы, где вас просят ввести личные данные: посмотрите на доменное имя, протокол https и значок замка;
- ✓ настройте двухфакторную аутентификацию во всех социальных сетях, где это возможно (см. Памятку).
- ✓ в настройках приватности запретите незнакомым людям оставлять комментарии и скройте свои публикации от них, чтобы избежать спама и оскорблений.

4. *Создание профиля знаменитости* – любимый исполнитель вдруг объявил сбор, например, на помощь какому-то человеку, или розыгрыш призов.

Что делать:

- ✓ проверьте, верифицирована ли страница известного человека, с которым вы хотите пообщаться в соцсетях, – надежные профили отмечены синей галочкой;
- ✓ проверьте дату создания профиля и всех постов, если фотографии загрузили два дня назад, наверняка его автор – мошенник; определить оригинальность фото можно с помощью функции «поиск картинок» в Google или Яндексе;
- ✓ просмотрите контент аккаунта: вредоносные ссылки или нецензурные выражения – повод «не дружить» с такой публичной страницей.
- ✓ проанализируйте активность: почитайте комментарии и изучите ленту и скорость ее наполнения – фейковые профили наполняются быстро,

причем наполняются они однотипными комментариями, а также подписываются на всех подряд.

Тесты и опросы в социальных сетях

Каждый из нас так или иначе встречал в ленте социальных сетей забавные тесты, предлагающие узнать свой психологический возраст, на персонажа какого сериала похожи или с каким знаком зодиака у нас наибольший процент совместимости. Ответы на эти вопросы вряд ли помогут нам в жизни, но такие тесты могут позволить злоумышленникам украсть ваши персональные данные либо деньги с электронных счетов.

Тесты оперируют базовыми данными из профиля социальной сети такими, как имя, количество фотографий, связи с друзьями, для чего просят дать разрешение на синхронизацию с вашим профилем (доступ к фото, данным профиля, постам на стене, списку друзей и другой личной информации). Эти, казалось бы, безобидные и ни о чем не говорящие данные, попадут в базу разработчика и впоследствии использоваться с неправомерными целями.

Следует помнить, что тесты, опубликованные в социальных сетях, размещаются на сторонних ресурсах, владельцы которых зарабатывают на размещении рекламы и монетизации самих тестов – от пользователя могут потребовать плату за получение результатов теста или его прохождение, либо предложить установить какое-либо приложение. Тесты намеренно делают с огромным количеством вопросов в расчете на то, что пользователю станет жаль потраченного времени, и он отправит «недорогую» СМС, стоимость которой на самом деле может оказаться намного выше заявленной, или СМС может понадобиться несколько.

Кроме перехода по ссылке, может возникать опасность осуществления атаки под названием «*кликджекинг*» – мошенническая схема, при которой злоумышленник может получить доступ к конфиденциальной информации или даже к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу. Принцип основан на том, что поверх видимой страницы располагается невидимый слой, в который и загружается нужная злоумышленнику страница, при этом элемент управления (кнопка, ссылка), необходимый для осуществления требуемого действия, совмещается с видимой ссылкой или кнопкой, нажатие на которую ожидается от пользователя. Возможны различные способы применения технологии – от подписки на ресурс в социальной сети до кражи конфиденциальной информации и совершения покупок в интернет-магазинах за чужой счет

Что делать:

- ✓ при разрешении доступа теста к профилю в социальной сети всегда внимательно читайте, доступ к какой информации запрашивается.
- ✓ регулярно проверяйте настройки вашего профиля в социальной сети: какие приложения к нему привязаны и на что они имеют права.

- ✓ не вводите в тестах и при переходе по ссылкам информацию о данных банковской карты, номера телефонов, пароли и другие персональные данные.
- ✓ использование и регулярное обновление антивируса предотвратит проникновение вредоносного элемента, если он действительно присутствует в тесте.
- ✓ тесты можно пройти в интернете, не устанавливая для этого отдельные приложения (часто можно увидеть запрос на установку).

Онлайн-игры: весело провести время и стать жертвой мошенников?

Компьютерные игры уже давно перестали быть чем-то необычным и загадочным и в них играет огромное количество человек по всему миру. По данным компании Microsoft, общая аудитория видеоигр составляет более трех миллиардов человек[6].

С развитием интернета появился отдельный класс компьютерных игр, в которые можно играть не только локально на своем компьютере или с партнером на одной клавиатуре, а с тысячами и десятками тысяч игроков со всей планеты.

Рост количества игроков в онлайн-играх влечет за собой и рост угроз, поскольку мошенники стараются извлекать максимальную выгоду из сложившейся ситуации. В онлайн-играх хранится не только игровая валюта и приобретенные игровые предметы, но настоящие деньги – все это вызывает у злоумышленников особый интерес.

Основные опасности в онлайн-играх

1) *Кража персональных данных* – пожалуй, самый распространенный вид онлайн-мошенничества.

2) *Кража денег*: игровая валюта, предметы игры и настоящие деньги в виртуальном кошельке – основной интерес мошенников. Специалисты предупреждают, что для геймера риск подвергнуться мошенничеству наиболее высок, когда он открывает счет для оплаты, без чего нередко многие игры вообще не «запускаются». 48% случаев мошенничества приходится как раз в момент оплаты.

3) *Кража аккаунта*: украв аккаунт, мошенники начинают шантажировать пользователя, требовать деньги за возврат аккаунта.

4) *Вредоносное программное обеспечение*. Например, пользователю предлагается скачать плагин для какой-то игры. Не подозревая подвоха, он переходит по ссылке на другой сайт, где запущено вредоносное программное обеспечение. Цель такого ПО – нанести ущерб безопасности и конфиденциальности устройства пользователя. Кроме того, в файлы игры могут быть встроены вирусы, и по незнанию пользователь может впустить их в свою систему во время установки.

5) *Нарушение приватности*. Сопоставив данные, полученные из игр и других источников, злоумышленники могут получить доступ к другим

[6] Источник: https://news.microsoft.com/2020/09/21/microsoft-to-acquire-zenimax-media-and-its-game-publisher-bethesda-softworks/

вашим учетным записям, например, в социальных сетях, а также зарегистрировать на ваше имя новые учетные записи или даже создать цифровые личности.

6) *Скрытые сборы*. Некоторые онлайн-игры выпускаются в условно бесплатной версии: часть контента предоставляется бесплатно, а для получения доступа ко всем возможностям и функциям необходимо заплатить. Для этого необходимо привязать банковскую карту к своей учетной записи, и оплата будет автоматически списываться с карты при покупке пользователем новых предметов или услуг.

Самые распространенные *мошеннические схемы:*

1. Перенаправление игроков на фейковые сайты, которые, как правило, выглядят, как настоящие сайты для покупки аддонов (экипировки, силы, новых способностей и прочее) и игровой валюты. На самом деле основная цель этих сайтов, как и любых фишинговых, – обманом заставить пользователя перевести деньги за товар, который он никогда не получит.

2. *Атаки на IP-адреса игроков (*уникальные адреса пользователя в интернете), узнав который, мошенники могут вычислить ваш фактический адрес, имя, фамилию и другую закрытую личную информацию. Имея эти данные, они могут украсть вашу финансовую информацию или игровые учетные данные.

3. Фишинговые рассылки, цель которых – обманом выведать у пользователя данные его учетной записи. Мошенники могут рассылать игрокам письма по электронной почте о необходимости подтвердить свои данные для входа в систему. Переходя по ссылке из такого письма, игроки попадают на поддельную страницу входа в систему, где их просят ввести текущий пароль и имя пользователя. В итоге учетные данные оказываются в руках мошенников.

А могут и направляться ссылки на вредоносное ПО, причем самым разнообразным способом:

- на форуме игроков (публикуются ссылки на вредоносную программу под видом ссылки на патч игры);
- в самой игре (проводятся рассылки ссылок на вредоносную программу под видом «нового патча»);
- по электронной почте (рассылается спам с самой вредоносной программой либо со ссылками на нее);
- вредоносные программы распространяются через файлообменные сети;
- используются уязвимости веб-браузеров (для загрузки вредоносных программ при посещении игровых сайтов.)
- чаще всего злоумышленники публикуют на игровом форуме или в игре ссылки на вредоносную программу с заманчивыми комментариями.

4. *Поддельные мобильные версии популярных онлайн-игр.* После загрузки такие приложения устанавливают вредоносное ПО на смартфоны или компьютеры жертв. Мошенники используют такое ПО для перехвата данных учетных записей, используемых для совершения покупок на популярных

игровых платформах и приставках. Далее эти данные используются для кражи конфиденциальной информации пользователя, включая данные банковской карты, домашнего адреса и номера телефона.

Основные правила безопасности в онлайн-играх

✓ Для совершения любых игровых покупок пользуйтесь только официальными сайтами, при этом внимательно проверяя доменное имя сайта, так как мошенники часто используют созвучные с брендом доменные имена.

✓ Узнавая о новой возможности в игре или приложении не из официального источника, поищите больше информации по этой теме. Чаще всего уже есть люди, которые с этим сталкивались и поделились своим положительным или отрицательным опытом.

✓ Ищите и проверяйте информацию об акциях и выгодных предложениях на официальных источниках или у официальных представителей.

✓ Никогда не переходите по ссылкам, ведущим на сторонние сайты.

✓ Не отвечайте на электронные письма или запросы на переписку**,** в которых вас просят указать банковские, финансовые или персональные данные, даже если вам кажется, что сообщение отправлено от игровой платформы. Настоящая компания не будет запрашивать у вас информацию через сообщения.

✓ Не делитесь персональной информацией, не передавайте данные учетной записи по интернету. Не пересылайте ваши учетные данные даже друзьям.

✓ Используйте надежный пароль для входа в игру и никогда не используйте один и тот же пароль для нескольких учетных записей.

✓ Не забывайте о двухфакторной аутентификации. Она надежнее защищает вас и усложняет злоумышленникам задачу.

✓ Не забывайте регулярно обновлять антивирусное ПО.

✓ Одним из способов защиты может быть VPN (Virtual Private Network, виртуальная частная сеть). Она делает ваше интернет-соединение приватным. VPN-приложения легко устанавливаются, не требуют сложной настройки и обладают рядом преимуществ:

- защищают от атак, например, DDoS, которые могут предприниматься против соперников в онлайн-играх, особенно в случае конкурентной борьбы;
- обеспечивают дополнительную безопасность при передаче данных и совершении банковских операций, поскольку VPN-соединение невозможно отследить.

Некоторые VPN-приложения распространяются бесплатно, однако они могут ограничивать передачу данных и не обеспечивать полноценную безопасность. Перед тем как выбрать VPN, нужно четко понимать, на что будет распространяться его защита. Для этого ознакомьтесь с условиями предоставления услуг, в том числе с политикой конфиденциальности. Несмотря на то что некоторые VPN-сервисы обещают защищать вас от вредоносного ПО и фишинговых сайтов, они не гарантируют такого же уровня

защиты, какой дает самостоятельный антивирус, поэтому оптимальный вариант – иметь и то, и другое.

РАЗДЕЛ III. Защита прав человека в финансовой сфере

Невозможно рассматривать вопросы защиты прав человека в финансовой сфере, не определив понятие собственно «прав человека». В их число принято включать право на жизнь и свободу, свободу от рабства и пыток, свободу убеждений и их свободное выражение, право на труд, образование и т.д. Этими правами должны обладать все без исключения люди вне зависимости от их пола, возраста, расовой и этнической принадлежности, вероисповедания и т.д.[7].

Перечень ключевых прав и свобод человека зафиксирован во Всеобщей декларации прав человека, принятой в 1948 году, позднее были созданы и другие документы, расширяющие и уточняющие перечень прав человека в различных сферах[8].

Многие из упомянутых выше прав человека с финансовой сферой напрямую не связаны, однако ошибочно было бы думать, что в финансовой сфере не могут нарушаться права человека. Среди факторов, непосредственно угрожающих правам человека в финансовом секторе[9], выделяются:

1. Дискриминация в практиках кредитования: выдача кредитов может затрагивать права человека вне зависимости от величины и срока займа. Так, в выдаче займа человеку может быть отказано из-за его расы, религии или вероисповедания. А развитие автоматической проверки кредитоспособности позволяет замаскировать такие практики.
2. Отсутствие объективного представления о клиенте: все финансовые организации должны проводить полный комплекс проверок до выдачи кредита, в том числе при работе с людьми. Несоблюдение этого принципа и выдача кредита без проверок может привести к серьезным нарушениям прав человека впоследствии.
3. Отсутствие объективного представления о секторе, в который планируется инвестировать: финансовые организации должны убедиться, что их инвестиции в разного рода проекты не ведут к нарушению прав человека.
4. Конфиденциальность данных клиентов и сотрудников: слабая защита такого рода информации может вести к нарушению прав человека, особенно в случае, если третьим лицам стала доступна информация о важных для человека аспектах его финансового положения. Финансовым организациям важно обеспечивать защиту данных, чтобы этого не произошло, а также повышать компетенции работников в части защиты информации.

---

[7] Права человека / Организация объединенных наций. URL: https://www.un.org/ru/global-issues/human-rights (дата обращения: 04.07.2022)

[8] Всеобщая декларация прав человека, 1948. / URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 04.07.2022)

[9] 10 Human Rights Priorities for the Financial Sector // BSR. URL: https://www.bsr.org/en/our-insights/primers/10-human-rights-priorities-for-the-financial-sector (дата обращения: 04.07.2022)

5. Равенство в оплате труда: организации в финансовом секторе (как и в любой другой сфере) должны обеспечивать справедливую оплату труда, основанную на оценке производительности работника, его профессиональных, а не каких-либо других качеств. В противном случае нарушается одна из базовых предпосылок концепции прав человека – идея о всеобщем равенстве.

Перечисленные выше возможности для нарушения прав человека в финансовой сфере демонстрируют, как эта область вписана в более широкую концепцию прав человека. Однако многие из аспектов, о которых шла речь, касаются, скорее, работников сферы финансов или межорганизационного взаимодействия.

Что касается специфических прав человека в сфере финансов, стоит отметить, что те, кто говорит о таких рода правах, апеллируют к статье 25 (1) Декларации прав человека, которая утверждает, что «Каждый человек имеет право на такой жизненный уровень, включая пищу, одежду, жилище, медицинский уход и необходимое социальное обслуживание, который необходим для поддержания здоровья и благосостояния его самого и его семьи, и право на обеспечение на случай безработицы, болезни, инвалидности, вдовства, наступления старости или иного случая утраты средств к существованию по не зависящим от него обстоятельствам». Они обращают внимание, что именно наличие финансов и доступ к финансовым инструментам (например, кредитованию) и позволяет человеку получить доступ ко всем базовым благам, на которые должен иметь право каждый. Более того, именно наличие возможности использовать финансовые инструменты может способствовать выходу из бедности (которая трактуется как отсутствие доступа к перечисленным выше благам). Исходя из этого, ученые делают вывод, что право на доступ к финансам и кредитованию надо рассматривать как право человека[10].

В обыденной жизни понятие прав человека в финансовой сфере может трактоваться более широко, и говоря о нарушении прав человека, эксперты зачастую понимают ситуации, когда граждане сталкиваются с финансовым мошенничеством, проблемами с кредитными организациями и пр., и оказываются вынужденными бороться за сохранность своих средств. Несмотря на то, что многое в части финансовой безопасности зависит от самого человека, важную роль в ее обеспечении играют организации, обеспечивающие защиту прав человека в финансовой сфере[11].

Меры по защите прав человека в финансовой сфере можно разделить на реактивные (работу по факту уже совершенного мошенничества, например, на основе жалоб от его жертв) и превентивные (когда потенциальные нарушения

---

[10] Pradeep K.B. Access to Finance and Human Rights / MPRA Paper No. 80336. 03.08.2017. URL: https://mpra.ub.uni-muenchen.de/80336/1/MPRA_paper_80336.pdf (дата обращения: 04.07.2022)

[11] Перечень организаций и описание их полномочий подготовлено на основе: Защита прав и интересов потребителей финансовых услуг. Федеральный фонд по защите прав вкладчиков и акционеров. URL: https://fedfond.ru/bitrix/docs/zaschita_prav.pdf?ysclid=l4orjbx4qj889467271 (дата обращения: 22.06.2022)

прав человека выявляются до того, как от них кто-то пострадал. Деятельность в обоих направлениях ведет *Банк России*[12]. В него можно обратиться и сообщить, что финансовая организация нарушает права человека в финансовой сфере. ЦБ не вмешивается в договорные отношения между организацией и клиентом, однако может инициировать проверку деятельности организации и принять меры, если нарушения будут выявлены. ЦБ ведет статистику по обращениям с жалобами на различные виды организаций. Более половины всех жалоб на нарушение прав человека в финансовой сфере приходится на кредитные организации. Всего же за январь-март 2022 года в Банк поступило 94,9 тыс. жалоб. Банк России имеет свою интернет-приемную, где можно выбрать удобный способ обращения за его помощью: https://cbr.ru/reception/.

Если Банк России не вмешивается в отношения клиента и организаций, то помочь с урегулированием конфликта может *финансовый омбудсмен*. Он является независимым от органов власти, организаций и должностных лиц. В случае возникновения спорных ситуаций с финансовой организацией он может помочь осуществить досудебное урегулирование и избежать обращения в суд. Существует ряд ограничений для тех, кто хочет обратиться за помощью к финансовому омбудсмену:

– он рассматривает вопросы оказания финансовых услуг для личных, семейных, бытовых нужд, не связанных с ведением бизнеса;
– все споры с финансовыми организациями решаются только при их взаимодействии с финансовым уполномоченным;
– максимальный размер денежных требований составляет 500 тыс. рублей (исключение – споры по ОСАГО, там лимит не установлен);
– со дня возникновения спора с финансовой организацией должно пройти менее трех лет.

Перед тем, как обратиться за помощью к финансовому омбудсмену, следует убедиться, что его спор подлежит рассмотрению, затем подать претензию в финансовую организацию и написать обращение финансовому уполномоченному.

Связаться с уполномоченным, а также найти более подробную информацию о работе финансового уполномоченного можно на официальном сайте: https://finombudsman.ru/.

Юридическую помощь в части урегулирования отношений с финансовыми организациями также оказывает *Общероссийская Общественная Организация «Союз защиты прав потребителей финансовых услуг» (Финпотребсоюз)*, созданная в 2010 году. Целью организации является защита прав и законных интересов потребителей в сфере финансовых услуг и создание справедливого и цивилизованного финансового рынка. Организация решает целый круг задач, связанных с оказанием юридической помощи, содействием повышению эффективности поставщиков финансовых услуг,

[12] Защита прав потребителей финансовых услуг // Банк России. URL: https://cbr.ru/protection_rights/ (дата обращения: 22.06.2022)

общественным контролем за соблюдением законодательства в данной сфере, повышением информированности о рынке финансовых услуг, предотвращением мошенничества и пр. Более подробную информацию и контакты организации можно найти на ее сайте: http://www.finpotrebsouz.ru/.

Еще одна организация, занимающаяся защитой прав человека – *Роспортебнадзор*, его задача – защита прав потребителей (в том числе потребителей финансовых услуг). Эта организация может осуществить проверку, соблюдает ли организация, оказывающая финансовые услуги, правила их предоставления. Помимо этого, Роспотребнадзор отвечает за проверку того, чтобы финансовая организация не предоставляла информацию, вводящую в заблуждение ее клиентов. В случае выявления каких-либо нарушений Роспотребнадзор может применить меры по их пресечению: выдать предписание о прекращении нарушения прав пользователей, потребовать устранить существующие нарушения, а также привлечь к ответственности тех, кто совершил нарушения. Он же ведет статистику относительно выявленных нарушений в сфере потребителей финансовых услуг.

Контакты горячей линии по защите прав потребителей, а также информацию о деятельности Роспотребнадзора можно найти на официальном сайте: https://www.rospotrebnadzor.ru/.

Федеральную антимонопольную службу можно также отнести к организациям, стоящим на страже прав человека в финансовой сфере. Одной из ключевых ее задач является обеспечение конкуренции на рынке финансовых услуг. Наряду с этим она контролирует соблюдение законодательство в сфере рекламы. В числе направлений деятельности:

– предотвращение и пресечение рекламы, способной ввести пользователя в заблуждение или нанести вред его здоровью;
– защита от недобросовестной конкуренции;
– привлечение субъектов рекламной деятельности к ответственности за нарушение законодательства;
– взаимодействие с органами регулирования рекламы.

Говоря об организациях, защищающих права потребителей финансовых услуг, нельзя не отметить работу *органов внутренних дел, полиции*. Они занимаются расследованием преступлений и обязаны принимать обращения граждан в любое время вне зависимости от места совершения преступления и полноты данных о нем. В заявлении нужно указать суть произошедшего, дату, время и место. Важно также предоставить информацию о размере нанесенного ущерба. После подачи заявления необходимо получить талон-уведомление о его приеме. Решение о дальнейшей судьбе заявление должно быть принято в течение семи дней с момента обращения. Если ответ не получен, нужно обратиться к руководителю ОВД, а если и у него ответ получить не удастся – в прокуратуру.

Существуют также организации, ориентированные на помощь потребителям отдельный категорий финансовых услуг. Так, например,

Федеральный фонд по защите прав вкладчиков и акционеров, работающий с 1995 года, решает следующие задачи:

– выплата компенсаций, пострадавшим на российском финансовом рынке;

– бесплатное юридическое консультирование пострадавших на российском финансовом рынке;

– повышение финансовой грамотности и финансовой бдительности.

Подробную информацию о деятельности фонда, а также о том, кто и в каком случае может рассчитывать на компенсацию можно найти на официальном сайте: https://fedfond.ru/

Защитой интересов вкладчиков занимается и *Агентство по страхованию вкладов*, созданное в 2004 году и оказывающее физическим лицам и индивидуальным предпринимателям помощь в получении средств, вложенных в банки (банк для этого должен быть участников системы страхования вкладов).

Проверить, какие банки являются участниками программы, а также узнать, что делать вкладчикам банков, лишившихся лицензии, также можно на официальном сайте агентства: https://www.asv.org.ru/

Прокуратура Российской Федерации играет особую правозащитную роль, так как ее органы обладают относительной автономностью функциональных ветвей государственной власти и достаточной разветвленностью, обеспечивающей практически повсеместный доступ к ним населения. В Федеральном Законе от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Фе-дерации» закреплены нормы, подтверждающие правозащитный характер деятельности органов прокуратуры. Кроме того, прокуратура обладает полномочиями по осуществлению защиты прав и свобод человека и гражданина, как в надзорном, так и в ненадзорном видах деятельности. Подать обращение в Прокуратуру РФ можно на сайте: https://epp.genproc.gov.ru/web/gprf/internet-reception.

Приложения

Приложение №1

Глоссарий

Аутентификация – это процедура проверки подлинности лица, получающего доступ к автоматизированной системе, путем сопоставления сообщенного им идентификатора и предъявленного подтверждающего фактора.

Блокчейн – распределенная база данных, которая содержит информацию обо всех транзакциях, проведенных участниками системы.

Доходы – совокупность всех денежных поступлений человека или домохозяйства (таких, как заработная плата, доходы от предпринимательской деятельности, социальные выплаты, доходы от собственности и пр.).

Доходы, полученные преступным путем – денежные средства или иное имущество, полученные в результате совершения преступления.

Инфляция – изменение в уровне цен в текущем периоде в сравнении с выбранным периодом.

Комплаенс контроль – система внутреннего обеспечения соответствия деятельности компании требованиям финансового законодательства.

Кредитование – предоставление заемщику денег банком или другой финансовой организацией под определенный процент.

Криптовалюта – цифровая платежная система, при проведении операций в которой не участвуют банки.

Легализация (отмывание) доходов, полученных преступным путем – придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Личная финансовая безопасность – это социально-экономическая возможность человека, иметь финансовую независимость для удовлетворения своих материальных и духовных потребностей, как индивидуально, так и внутри общества, а также сохранение этой независимости в перспективе и её дальнейшее преумножение.

Мошенничество – хищение путем обмана или злоупотребления доверием.

Национальная финансовая безопасность – состояние финансово-кредитной сферы, которое характеризуется сбалансированностью, устойчивостью к внутренним и внешним негативным воздействиям, способностью этой сферы обеспечивать эффективное функционирование национальной экономической системы и экономический рост; уровень защищенности финансовых интересов на макро- и микроуровнях финансовых отношений.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Сбережения – разница между доходами и расходами населения.

Фальшивомонетничество – изготовление в целях сбыта поддельных банковских билетов, ценных бумаг, а также их хранение и перевозка.

Финансовая безопасность – понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне.

Фишинг – рассылка электронных писем о якобы производимых изменениях в системе безопасности банка.

Форекс – рынок, где происходит покупка и продажа денежных знаков.

Ресурсы

1. Курс по анонимности и безопасности в сети. URL: https://book.cyberyozh.com/ru/?fl=ru.
2. Агентство по страхованию вкладов [сайт]. URL: https://www.asv.org.ru/.
3. Федеральный фонд по защите прав вкладчиков и акционеров [сайт]. URL: https://fedfond.ru/.
4. Роспортебнадзор [сайт]. URL: https://www.rospotrebnadzor.ru/.
5. Общественная Организация «Союз защиты прав потребителей финансовых услуг» (Финпотребсоюз) [сайт]. URL: http://www.finpotrebsouz.ru/.
6. Финансовый омбудсмен [сайт]. URL: https://finombudsman.ru/.
7. Центральный Банк (Банк России) [сайт]. URL: https://cbr.ru/reception/.
8. Портал «Финансовая культура»: https://fincult.info/.
9. Портал «Финграмота»: http://www.fingramota.org/.
10. Статистика интернета и соцсетей на 2023 год — цифры и тренды в мире и в России [сайт]. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/.
11. Интернет-портал Национального агентства финансовых исследований. URL: https://nafi.ru/analytics/27-derzhateley-bankovskikh-kart-mogut-stat-zhertvami-moshennikov/.
12. Информационно-просветительский ресурс Центрального банка Российской Федерации «Финансовая культура». URL: https://fincult.info/articles/ostorozhno-moshenniki/.
13. Официальный сайт Министерства финансов Российской Федерации. URL: https://minfin.gov.ru/ru/om/fingram/directions/strategy/.
14. Портал Некоммерческого партнерства «Институт образования и науки» (НП «ИОН»). URL: https://profin.top/literacy/lichnye-finansy/base.html.
15. Видеоуроки финансовой грамотности для школьников. URL: https://www.youtube.com/watch?v=kK5vp_uzY6Q.
16. Научно-образовательный портал «IQ» Национального исследовательского университета «Высшая школа экономики». URL: https://iq.hse.ru/more/finance/neobhodimost-povishenia-finansovoj-gramotnosti.

Тестовые задания для контроля знаний

1. **К вам в «друзья» добавляется незнакомый человек. Ваши действия (1 верный ответ).**
   a) Отклоню его заявку.
   b) Добавлю, если у нас есть общие друзья.
   c) Добавлю в друзья! Главное - побольше друзей!
   d) Посмотрю его страничку и добавлю в друзья, если не увижу ничего подозрительного.
2. **Ваш близкий друг прислал вам письмо следующего содержания: «Привет. В этом месяце не выплатили зарплату, а у меня кредит. Дай тысячу в долг. Скинь на карту. Ваши действия (1 верный ответ).**
   a) У меня у самого денег нет, не стану переводить.
   b) Не стану давать в долг, пока не поговорю с другом лично.
   c) Первый раз в долг просит. Сумма небольшая, почему бы не выручить друга. Переведу!
   d) Не помню, чтобы друг рассказывал мне о кредите. Уточню в переписке, что за кредит и когда он его оформил. После ответа переведу необходимую сумму.
   e) В долг не дам, знаю, что точно не вернет!
3. **Вы подписаны на официальный аккаунт известного блогера, который только что опубликовала пост: «В честь моего дня рождения я решил разыграть айфон. Для участия в розыгрыше перейдите по ссылке и заполните ваши данные». Ваши действия. (1 верный ответ).**
   a) Не стану переходить по ссылке и открывать ее.
   b) Буду участвовать, мне как раз нужен новый телефон.
   c) Сначала проверю, не фейковый ли это аккаунт: если есть «синяя галочка» рядом с ником, то приму участие. Все безопасно!
4. **Вы увидели на странице своего друга репост с просьбой о финансовой помощи на операцию тяжелобольному ребенку. В профиле ребенка указаны все документы, подтверждающие диагноз и необходимость срочной операции. Вы поможете? (1 верный ответ).**
   a) Переведу деньги и сделаю репост на своей страничке. Ребенку обязательно надо помочь!
   b) Это скорее всего мошенники, помогать не стану. Лучше помогу кому-нибудь через проверенный благотворительный фонд.
   c) Посмотрю внимательно все документы, подтверждающие диагноз. Если ситуация действительно тяжелая – отправлю небольшую сумму.
   d) Мой друг помог, и я помогу! Это улучшит мою карму.
5. **Часто под видом интернет-магазинов в социальной сети скрываются мошенники, поэтому перед совершением покупки необходимо тщательно изучить страничку магазина. Выберете в каком магазине вы не станете совершать покупку? (1 верный ответ).**
   a) Если у магазина нет своего сайта.
   b) Если у магазина нет возможности оплатить товар при получении.
   c) Если у магазина мало подписчиков и нет отзывов покупателей.
   d) Если у магазина нет возможности самовывоза.
6. **Вы активно общаетесь в разных социальных сетях, но одной уже долгое время не пользуетесь. Как вы поступите с вашим аккаунтом? 1 верный ответ.**
   a) Не буду удалять, вдруг, еще пригодится!
   b) Не знаю, что с ним делать.
   c) Удалю его, зачем он мне, я им все равно не пользуюсь.
   Хочу удалить, но постоянно забываю об этом.
7. **Вы получили сообщение в социальной сети с предложением купить атрибуты для онлайн-игры по очень привлекательным ценам и ссылкой на ресурс, где их можно купить. Ваши действия (1 верный ответ).**
   a) Экономия – это всегда хорошо! Обязательно пройду по ссылке и, если цены меня устроят, сделаю покупку.
   b) Это все проделки мошенников, не буду переходить по ссылке.

c) Перейду по ссылке, боюсь упустить хорошую возможность!

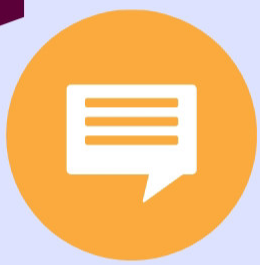
8. **Что способствует понижению личной финансовой безопасности человека? (выберите все подходящие варианты ответа)**
   a) Мошеннические действия со стороны злоумышленников
   b) Низкий уровень финансовой грамотности
   c) Ухудшение экономической ситуации
   d) Длительная занятость на одном рабочем месте
9. **Какие из приведенных ниже примеров характеризуют ситуацию диверсификации рисков? (выберите все подходящие варианты ответа)**
   a) Распределение всех имеющихся сбережений между счетами в различных банках и в различных валютах
   b) Игнорирование информации о рисках отзыва лицензии у крупного банка
   c) Увеличение риска угона автомобиля из-за хранения его у дома, а не на платной стоянке
   d) Использование различных инвестиционных инструментов: акций, облигаций и инвестиций в недвижимость
10. **Какие действия по защите интересов потребителей финансовых услуг может предпринимать Банк России? (выберите все подходящие варианты ответа)**
    a) Осуществление проверок деятельности финансовых организаций при получении жалоб от граждан
    b) Обращение в суд с требованием принудить финансовую организацию вернуть средства, переданные ей потребителем
    c) Публикация информации о деятельности организаций, нарушающих права человека в финансовой сфере
    d) Выплата компенсаций пострадавшим от действий финансовых мошенников
11. **В каком случае финансовый омбудсмен не сможет оказать помощь в досудебном урегулировании претензий к финансовой организации? (выберите все подходящие варианты ответа)**
    a) Если с момент возникновения спора прошло менее 3 лет
    b) Если финансовые услуги тому, чьи права были нарушены, оказывались для ведения бизнеса
    c) Если претензия к организации связана со спорами по обязательному страхованию автогражданской ответственности (ОСАГО)
    d) Если обращение было направлено финансовому омбудсмену в электронной форме

Ответы: ***1*** *– a)* ***/ 2*** *– b* ***/ 3*** *– c* ***/ 4*** *– b* ***/ 5*** *– b* ***/ 6*** *– c* ***/ 7*** *– b* ***/ 8*** *– a b c* ***/ 9*** *– a d* ***/ 10*** *– a c* ***/ 11*** *– b*

Что делать в случае утечки персональных данных?

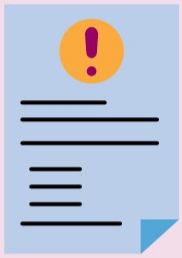
В случае, если ваши персональные данные попали в сеть и оказались выложены на одном или нескольких сайтах, эффективными могут быть следующие меры.

01



Обратитесь к владельцу сайта

02



Напишите заявление в уполномоченные органы

03



Обратитесь в суд

04



Замените документы

Помните: утечку легче предотвратить, чем устранять ее последствия!

Как предотвратить кражу цифровой личности?

Правила цифровой гигиены

- не делиться о себе большим количеством информации в сети;
- создавать сложные и разные пароли, пользоваться менеджером паролей для их создания и хранения;
- везде, где это возможно, настроить двухфакторную авторизацию для входа в аккаунт;
- устанавливать приложения только из официальных магазинов и внимательно проверять, какие разрешения вы даёте установленным приложениям;
- не переходить по сомнительным ссылкам;
- использовать для передачи почтовые сервисы с возможностью удалить данные у получателя;
- обязательно удалять из электронного почтового ящика и мессенджеров письма с персональными данными;
- не называть ксерокопии документов ключевыми словами при пересылке;
- не использовать социальные сети для авторизации на сайтах;
- удалять все неиспользуемые аккаунты;
- при пересылке копий своих документов, указывать на них дату и адресата (либо сайт, куда отправляете данные) с помощью водяного знака или приложенной к фото документов записки.

Двухфакторная аутентификация

метод проверки, который позволяет установить, что в аккаунт действительно входит его владелец через **дополнительное** подтверждение различных типов данных (факторов)



1 фактор

то, что мы знаем
(пароли, кодовые слова и фразы)



2 фактор

то, что мы имеем
(дополнительное устройство, на которое придет код подтверждения)



3 фактор

то, что присуще только нам
(биометрические персональные данные)

подключенная двухфакторная аутентификация значительно усложнит работу мошенникам, так как, помимо пароля, им потребуется заполучить доступ к вашим смс, почте или даже устройству.

- Настоить двухфакторную аутентификацию можно в настройках безопасности
- Если вам на мобильный телефон внезапно пришло уведомление о попытке входа в ваш аккаунт – немедленно смените пароль от аккаунта
- В случае утери телефона звоните мобильному оператору и блокируйте сим-карту