Рекомендации по работе с презентацией Тематического урока «Финансовая безопасность личности в сети Интернет»

Цель: создание условий для формирования у обучающихся базовых представлений об основах финансовой безопасности.

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, закрепить базовые финансовые понятия, отработать алгоритм решения сложных жизненных ситуаций, связанных с опасностью стать жертвой финансовых пирамид;
- сформировать у обучающихся общее представление о финансовых рисках в современной экономической ситуации; понимание опасности финансовых пирамид и способов их распознавания; понимание системной взаимосвязи личной финансовой безопасности и финансовой безопасности государства; понимание опасности для государства и граждан преступлений в сфере финансов.

Методический материал носит рекомендательный характер; преподаватель, принимая во внимание особенности обучающихся, может варьировать задания, их количество, менять этапы занятия.

Слайд	Комментарий для учителя
СЛАЙД 1 	*Согласно статистическим данным Национального агентства финансовых исследований (НАФИ)[1], 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%).* ***Финансовая безопасность** – понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне. Из определения данного понятия мы можем выделить уровни финансовой безопасности:* • *национальный, то есть финансовая безопасность всего государства;* • *региональный – безопасность отдельных частей государства;* • *корпоративный, то есть финансовая безопасность организаций;*

[1] 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).

Министерство образования и молодежной политики СО
28.02.2023
Вх.№ 4428

СЛАЙД 2



СЛАЙД 3



СЛАЙД 4



- *личный – финансовая безопасность отдельно взятого индивида, или личная финансовая безопасность.*

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. Иными словами, финансовая безопасность личности означает независимость и стабильность – и именно поэтому так важно знать, как ее обеспечить каждому из нас.*

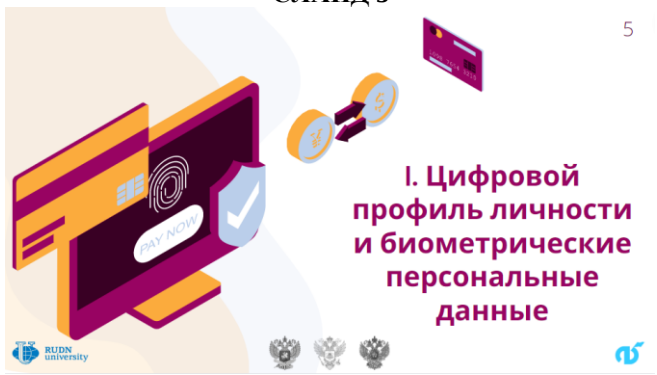
Финансовая безопасность государства *– понятие более широкое. Она представляет собой состояние финансово-кредитной сферы, которое характеризуется сбалансированностью, устойчивостью к внутренним и внешним негативным воздействиям, способностью этой сферы обеспечивать эффективное функционирование национальной экономической системы и экономический рост; уровень защищенности финансовых интересов на макро- и микроуровнях финансовых отношений. Достичь этого можно лишь обеспечив должный уровень финансовой безопасности личности и организаций.*

Задание

Проанализируйте данные на слайдах 2-4 и ответьте на вопросы.

1. Прокомментируйте данные диаграммы на слайде №2. Какие выводы можно сделать из приведенной информации?
2. Изучите слайд №3. Что такое личная финансовая безопасность? Связана ли личная финансовая безопасность с национальной? Обсудите.
3. Нужно ли современному человеку учиться финансовой безопасности и финансовой грамотности? Назовите не менее трех причин, обосновывающих важность финансовой грамотности для вас.
4. Опираясь на информацию слайда №4, ответьте на вопрос: как, по вашему мнению, связаны финансовое мошенничество и финансовая безопасность? Свой ответ обоснуйте.

СЛАЙД 5



СЛАЙД 6



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[2] 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.

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 Москвы (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).

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 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

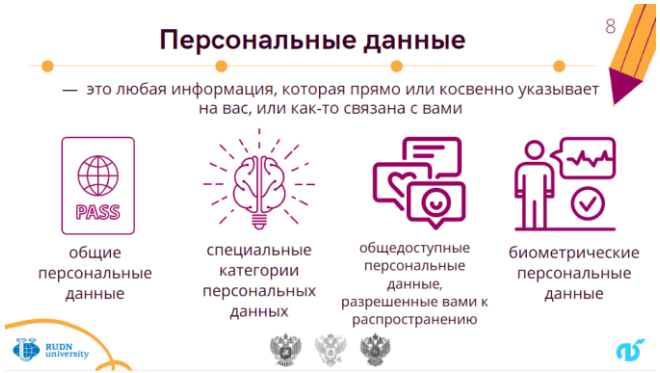
[2] Уровень цифровой грамотности подростков составляет 73 п.п. из 100, для сравнения — индекс взрослых равен 52 п.п./

[3] Всероссийский репрезентативный опрос молодежи проведен Аналитическим центром НАФИ 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).

СЛАЙД 7



СЛАЙД 8



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).

Задание:

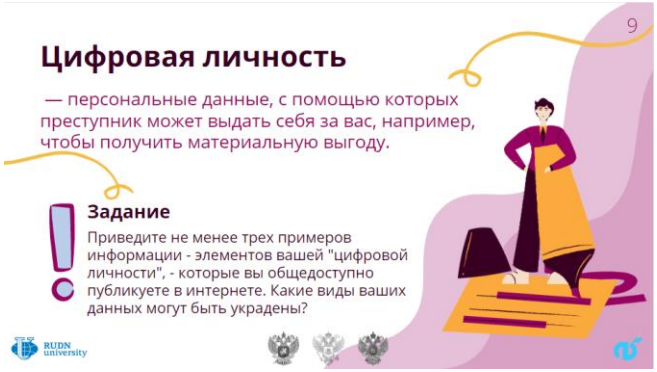
1. Изучите слайды №6-7 и ответьте на вопросы. Прокомментируйте данные диаграмм. Какие выводы можно сделать из приведенной информации? Считаете ли вы, что обладаете достаточными знаниями и навыками, чтобы защитить свою персональную информацию в сети Интернет?
2. Чем опасна утечка ваших персональных данных?
3. Слайд №8. Как вы думаете, что подразумевается под приведенными видами персональных данных?
4. Приведите примеры каждого из видов персональных данных.
5. Подумайте, как связана ваша личная финансовая безопасность с безопасностью ваших персональных данных в сети Интернет?

I. *Цифровой профиль человека 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

СЛАЙД 9



СЛАЙД 10



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.

*Кража цифровой личности – **фото, видео с ваших страниц в социальных сетях, аккаунтов и профилей, паспортных данных и копий документов** – 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.*

В случае, если вам кажется, что кража цифровой личности – это что-то из фантастических фильмов про будущее: 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.

Конечно, стать жертвой злоумышленников могут и те пользователи, которые не выставляют важные данные на всеобщее обозрение. Каждый десятый ребёнок сталкивался с мошенничеством с использованием фальшивых сайтов/писем. Например, они заходят на фейковые страницы для онлайн-покупок, заманивающие акциями и скидками, или попадаются на объявления о быстром заработке, цель которых, наоборот, выманить деньги, а не дать возможность их получить. Любой пользователь может стать жертвой утечки данных, когда учётные записи оказываются в сети из-за технической уязвимости или действий злоумышленников.

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**. Фото и видео реального, человека могут быть использованы для создания поддельной странички в социальных сетях и использования ее в качестве инструмента вымогательства денег.*

	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 красивых девушек 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. Но не только красивые девушки интересны мошенникам, любые краденные данные могут быть использованы для создания страничек. 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 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 парни, желая отомстить девушке, выставляли ее фотографию и анкету на различных 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. **Задание:** 1. Слайд №9. Приведите не менее трех примеров информации – элементов вашей «цифровой личности», – которые вы общедоступно публикуете в интернете. 2. Изучите информацию на слайде №10. Подумайте и назовите способы неправомерного использования вашей цифровой личности, не перечисленные на слайде.
СЛАЙД 11 	***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

СЛАЙД 12



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.*

Задание:

1. Изучите ситуацию, описанную на слайде №11.
2. Предположите, какие именно «детали семейной жизни» депутата В.В.Умнова могли быть опубликованы вместе с отзывами о товарах.
3. Опираясь на материалы Памятки о способах устранения последствий утечки данных (см. Приложение №4 к Методическим рекомендациям) и на образец обращения на слайде №12 составьте гипотетическое обращение гражданина В.В.Умнова к владельцам сайтов с просьбой об удалении незаконно размещенных персональных данных.

СЛАЙД 13



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, можно удалить отправленное письмо, можно запретить копирование и пересылку данных;* ✓ *обязательно удалять из электронного почтового ящика письма и мессенджеров, 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.* **Задание:** 1. Изучите правила цифровой гигиены, представленные на слайде №13 / в Памятке с правилами цифровой гигиены (см. Приложение №5 к Методическим рекомендациям). Обсудите в классе, какие из этих правил вы соблюдаете регулярно, а о каких впервые слышите.
	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

СЛАЙД 14



СЛАЙД 15



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.*

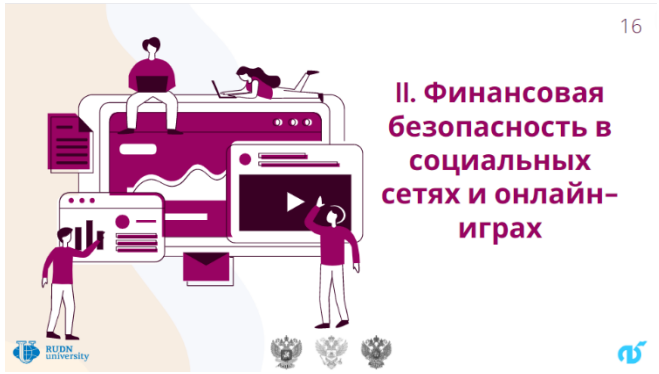
Дипфейки может создавать практически каждый в силу доступности обучения и количества программ для работы с этой технологией. Такой низкий порог входа двигает технологию вперед, но также увеличивает количество инструментов у мошенников для обмана пользователей и кражи их персональных данных.

Дипфейки могут быть использованы для манипулирования нашим сознанием: 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 соцетях 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.* **<u>Задание:</u>** 1. Проанализируйте ситуацию Марии, изложенную на слайде №15. 2. Как вы думаете, можно ли было избежать потери денег? 3. Какие меры предосторожности могла бы предпринять Мария, чтобы не стать жертвой мошенников? Сформулируйте последовательность своих действий в подобных ситуациях. <u>Предполагаемая модель ответа:</u> *В первую очередь необходимо прекратить разговор и позвонить тому человеку, о котором идёт речь. Если дозвониться ему не удалось, нужно постараться связаться с другими людьми, которым может быть известно его местонахождение (коллеги, друзья, родственники) для уточнения информации.* *Вероятнее всего, на данном этапе вы можете убедиться в том, что вас пытаются обмануть.* *Несмотря на волнение за родственника или близкого человека, нужно понимать: если незнакомец звонит вам и требует привезти на некий адрес деньги – это мошенник.* ***Если вам позвонил якобы близкий родственник или знакомый** и сообщил о том, что у него проблемы и ему грозит привлечение к уголовной ответственности, и он просит передать деньги сотруднику полиции, готовому урегулировать вопрос, нужно задать уточняющие вопросы: «Какая кличка у моей собаки» или «Когда и где мы виделись последний раз?», то есть необходимо задавать такие вопросы, ответы на которые знаете только вы оба.*

	***Если вы разговариваете якобы с сотрудником полиции**, уточните, из какого он отделения, после чего позвоните в дежурную часть данного отделения и поинтересуйтесь, действительно ли ваш родственник или знакомый доставлен именно туда.*
СЛАЙД 16  **СЛАЙД 17** 	***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[4]. 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 и сообщением «максимальный репост». Главное – создать конверсию поста и его*

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

СЛАЙД 18



СЛАЙД 19



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.*

Задание:

1. Ознакомьтесь с информацией, представленной на слайде №18, и ответьте на вопросы.
2. Случалось ли вам сталкиваться с одним из видов фишинга в социальных сетях? Если да, сумели ли вы распознать мошенничество или не задумались о возможном обмане?
3. Сформулируйте совместно с одноклассниками 1-2 правила, которые помогут распознать каждый из указанных видов фишинга и не стать жертвой мошенников.

Предполагаемые правила (возможные ответы обучающихся):

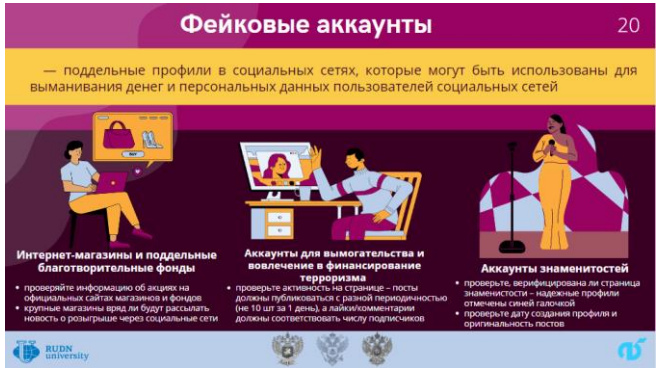
1. Просьбы друзей помочь с деньгами:

- позвоните вашему другу и спросите, действительно ли ему нужны деньги;
- никогда не переводите деньги на незнакомые номера без подтверждения от друга;
- проверьте, есть ли другая подозрительная активность на страничке вашего друга.

2. Псевдоблаготворительность:

При переводе денежных средств на нужды благотворительности следует обращать внимание на:

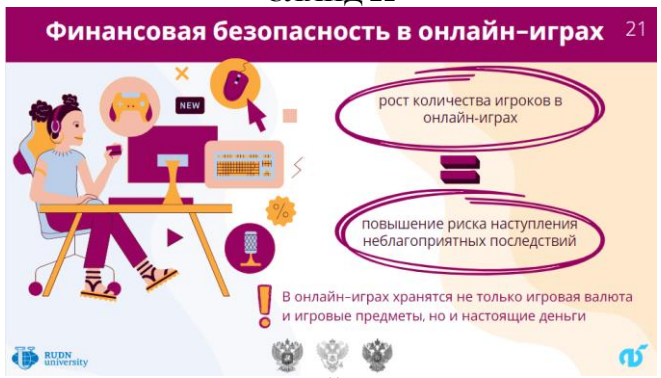
- то, сколько времени существует страничка;
- качество и количество контента;
- излишнее давление на жалость;
- перевод денег на личную карту;

	- срочность сбора; - реакция на уточняющие вопросы; - наличие ссылки на сайт благотворительного фонда (либо на то, является ли ссылка подлинной). 3. Смешные видео, громкие новости и иные сообщения, предполагающие переход по внешним ссылкам: - установите настройки приватности, чтобы вам могли отправлять сообщения только ваши друзья; - если вы получили такое сообщение от друга – позвоните ему по телефону и убедитесь, что его страничку не взломали; - не нажимайте на подозрительные ссылки; - при подключении к соцсети, проверьте, что адрес страницы указан верно; - не доверяйте громким заголовкам в постах в ленте; - обращайте внимание на адрес страницы, на которую вы переходите. 4. Изучите ситуацию, представленную на слайде №18. Какие из сформулированных вами ранее правил применимы к данной ситуации и могли бы предотвратить ее? 5. Слайд №19: работа с чек-листом «Защищен ли я от фишинга?». Отметьте, сколько правил защиты от фишинга вы соблюдаете регулярно.
СЛАЙД 20 	***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 и страницы поддельных благотворительных фондов для помощи попавшим в беду.*** *Такие магазины часто предлагают популярные или дефицитные товары по очень низким ценам, и обычно просят перевести полную стоимость прежде, чем отправят товар. А за фасадом благотворительного фонда могут скрываться террористические или экстремистские группировки, которые занимаются сбором денежных средств на финансирование своей противозаконной деятельности. 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. С таких аккаунтов,*

	если они принадлежали девушке, могут осуществляться попытки познакомиться с противоположным полом с целью выманивания денег и личных данных. Но чаще мошенники отправляют всем друзьям письма с просьбой о финансовой помощи или просто выручить деньгами до завтра. Кроме того, с таких аккаунтов может осуществляться деятельность по вовлечению пользователей социальных сетей в финансирование террористической и экстремистской деятельности. 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 – Приложение №6 к Методическим рекомендациям).* ✓ *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.*
	Финансовая безопасность в онлайн-играх *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*[5]*.* *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.*

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

СЛАЙД 21



СЛАЙД 22



СЛАЙД 23



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 ПО

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 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.

Задание:

1. Слайд №24: прочитайте текст на слайде №25. Проанализируйте ситуацию Артура.
2. Что было дальше? Предположите дальнейшее развитие событий, опираясь на свои знания о возможных видах мошенничества в онлайн-играх.
3. Какие выводы можно сделать из данной ситуации?

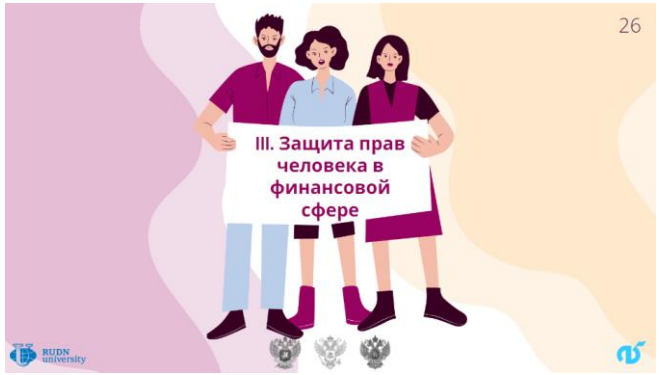
Артур, 20 лет:

«В бытность школьником нашел в «Counter-Strike: Source» какой-то сервер, где был чувак в скине Железного человека. Когда он умирал, его регдолл при этом издавал клевые металлические звуки — в общем, я был под впечатлением. Я спросил в общем чате, как получить такой скин, и админ сервера ответил, что модель доступна только для админов, но предложил ее за просто так.

СЛАЙД 24  **СЛАЙД 25** 	Он активировал скин для меня на сервере, и все вроде нормально работало, но потом он написал, что модель, дескать, нужно активировать в Steam, чтобы не исчезла. По его просьбе я поставил TeamViewer и дал доступ к компьютеру. Он подключился, открыл Блокнот прямо на моем рабочем столе, и там писал, что делать. <u>Предполагаемая модель ответа:</u> Пользуясь открытым доступом к компьютеру, мошенник зашел в игровую учетную запись Артура, чтобы якобы активировать скин. Артур предоставил ему все данные и коды с почты, потеряв свой аккаунт в Steam. <u>Выводы из ситуации:</u> Ставить стороннее программное обеспечение, а тем более передавать управление компьютером незнакомцам – большой риск. Нельзя сообщать незнакомым людям логин и пароль от своего игрового аккаунта, даже если они предлагают помощь / совет / игровые товары / обещают настроить крутую фичу или исправить серьезную проблему, как часто делают мошенники из фейковой техподдержки. Если вам нужна помощь технически подкованного товарища, пусть словами объяснит, как решать проблему, но на своем компьютере выполняйте инструкции самостоятельно.
	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[6].

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

СЛАЙД 26



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[7].

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[8], *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.*
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.*

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 прав человека выявляются до того, как от них кто-то пострадал. Деятельность в обоих направлениях ведет ***Банк России***[9]. *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*

[7] Всеобщая декларация прав человека, 1948. /
URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 04.07.2022)
[8] 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)
[9] Защита прав потребителей финансовых услуг // Банк России. URL: https://cbr.ru/protection_rights/ (дата обращения: 22.06.2022)

СЛАЙД 27



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, 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 – ***Роспотребнадзор****, 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 Федерации» 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.
СЛАЙД 28 	**<u>Подведем итоги. Задание:</u>** 1. Ответьте на вопросы, представленные на слайде №28. <u>Ответы:</u> *1 – a), b), c), e);* *2 – a), c);* *3 – a), c)* 2. Решите тестовые задания (см. Приложение №3 к Методическим рекомендациям) <u>Ответы:</u> *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*
СЛАЙД 29 	***Ознакомление обучающихся с возможностью принять участие в Международной олимпиаде по финансовой безопасности.***

СЛАЙД 30



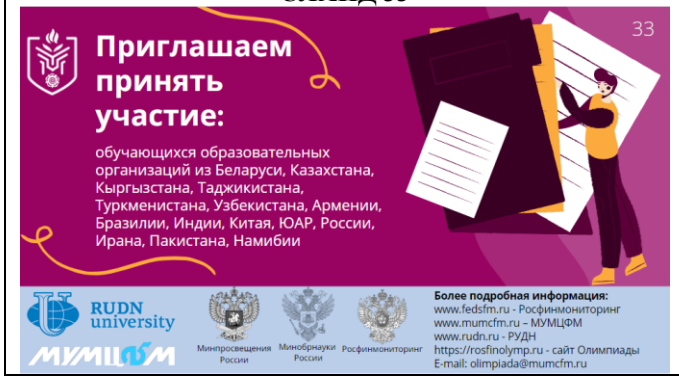
СЛАЙД 31



СЛАЙД 32


32
Приглашаем принять участие:
обучающихся образовательных организаций из Беларуси, Казахстана, Кыргызстана, Таджикистана, Туркменистана, Узбекистана, Армении, Бразилии, Индии, Китая, ЮАР, России, Ирана, Пакистана, Намибии
RUDN university
МУМЦФМ
Минпросвещения России
Минобрнауки России
Росфинмониторинг
Более подробная информация:
www.fedsfm.ru - Росфинмониторинг
www.mumcfm.ru – МУМЦФМ
www.rudn.ru - РУДН
https://rosfinolymp.ru - сайт Олимпиады
E-mail: olimpiada@mumcfm.ru

СЛАЙД 33


33
Приглашаем принять участие:
обучающихся образовательных организаций из Беларуси, Казахстана, Кыргызстана, Таджикистана, Туркменистана, Узбекистана, Армении, Бразилии, Индии, Китая, ЮАР, России, Ирана, Пакистана, Намибии
RUDN university
МУМЦФМ
Минпросвещения России
Минобрнауки России
Росфинмониторинг
Более подробная информация:
www.fedsfm.ru - Росфинмониторинг
www.mumcfm.ru – МУМЦФМ
www.rudn.ru - РУДН
https://rosfinolymp.ru - сайт Олимпиады
E-mail: olimpiada@mumcfm.ru