Общие вопросы цифровых угроз

теория и профилактика

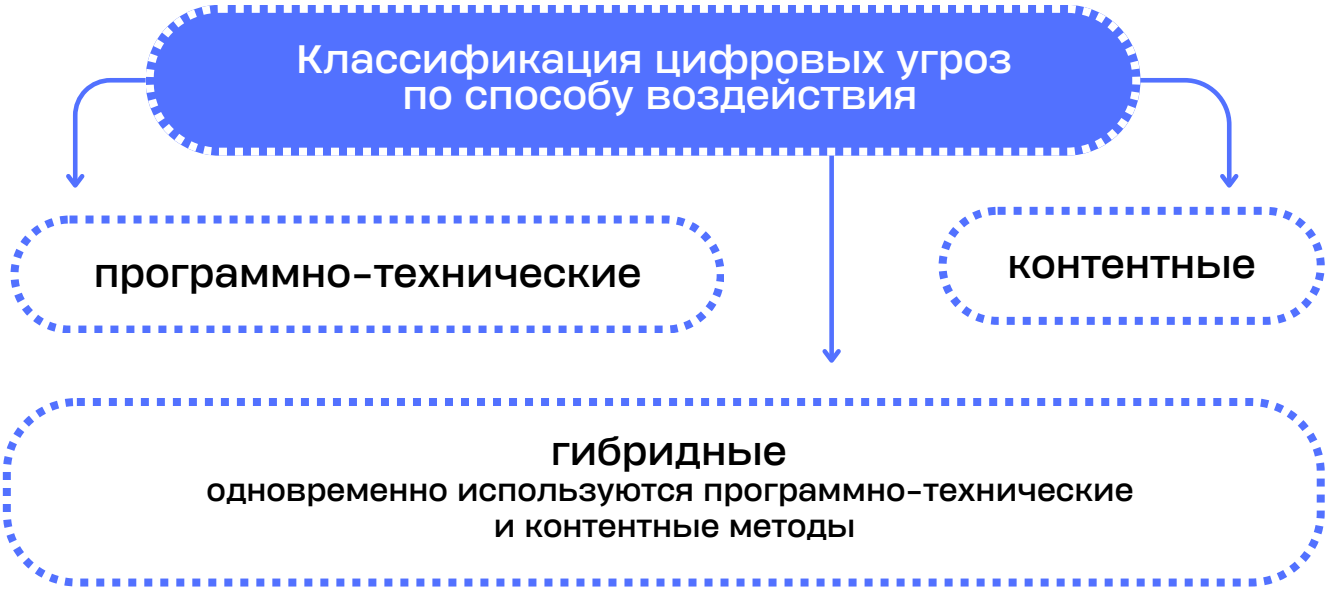
КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Урван Парфентьев
Координатор Центра Безопасного Интернета в России

термины и классификация

Цифровая угроза – это термин, скажем так, с двумя значениями.

- С одной стороны, его используют для обозначения некоего вида цифровой опасности как явления *(например, «популярной цифровой угрозой является киберунижение»)*
- С другой, цифровой угрозой могут назвать и конкретное цифровое преступление *(например, «цифровая угроза моему аккаунту»)*
- В качестве синонимов могут использоваться слова **инцидент** и **атака**. Правда, в последнем случае с уклоном в «программно-техническое вмешательство со злым умыслом».



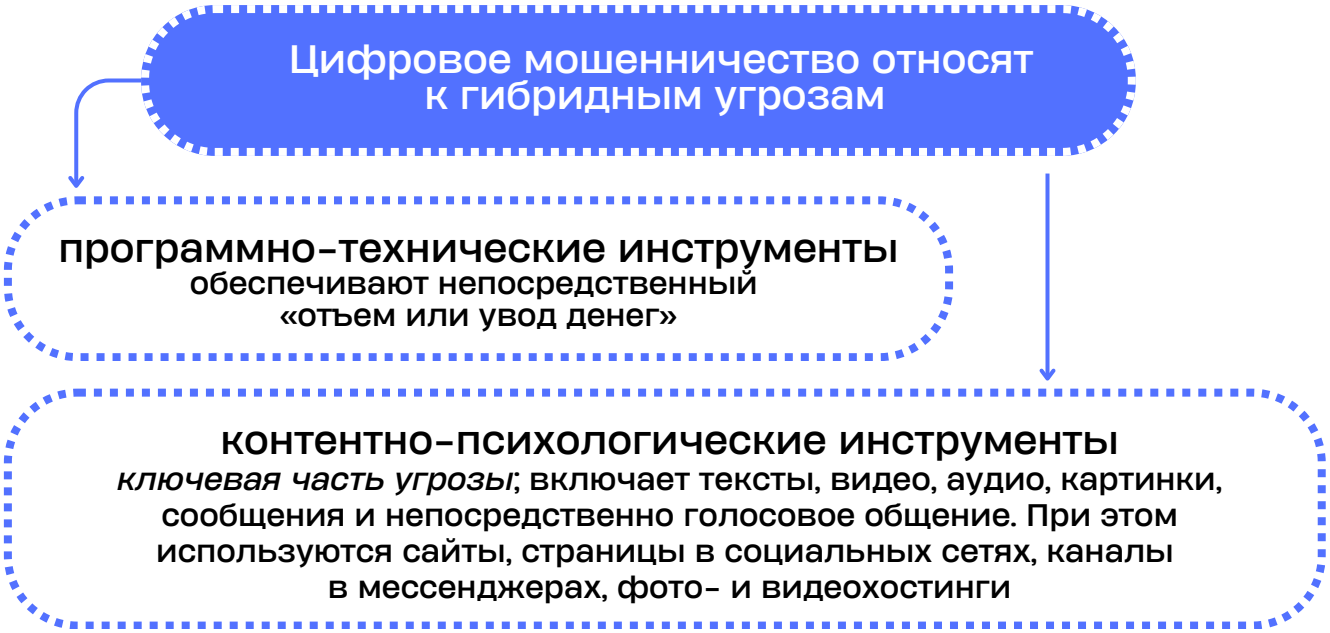
Типы угроз адаптируются к цифровому прогрессу, появлению новых технологий и возможностей.

«Кибербезопасность», «цифровая безопасность», «информационная безопасность» – эти понятия часто используются как синонимы, однако это немного не так.

- **Кибербезопасность** – это, скорее, понятие про безопасность программно-техническую, цифровых устройств и сетей.
- **Информационная безопасность** — это безопасность, связанная с оборотом информации, то есть всего того, что мы видим, слышим и публикуем в цифровом мире.
- К информационной близка по значению **контентная безопасность**; это понятие касается не только цифровой среды, но и книг, журналов, радио и телевидения.
- **Цифровая безопасность** – самое широкое из понятий, и включает безопасность в цифровой среде вообще: как программно-техническую, так и информационную.

цифровое мошенничество

- **Цифровое мошенничество** – наиболее известная *(читай – массовая)* интернет-угроза, которая означает, что деньги или что-то иное, имеющее ценность, попадает от жертвы злоумышленнику путем обмана или злоупотребления доверием.



основные характеристики и признаки

Данная угроза исключительно адаптивна: злоумышленники легко используют громкие информационные поводы, новые сервисы и технологии. **В целом можно выделить два основных сценария**:

1. **«Добрый волшебник»**: рассчитан на создание сверхвосторженного восприятия жертвой сделанного для нее предложения.

   Мошенник предлагает жертве некий значимый материальный бонус: существенную скидку за товар или услугу, возможность получения легкого дохода *(например, приглашение в «онлайн-казино», «письмо наследнику», «скидка» от онлайн-магазина, мобильного оператора или сетевой игры, «легкая подработка» из дома)* за несоразмерно большое вознаграждение.

2. **«Страх»:** построен на задаче устрашения жертвы.

   Типичные примеры: необходимость уплаты некоего «штрафа», «задолженности» под угрозой мгновенных «санкций» (*часто обращение исходит от имени «государственного органа» или иной известной организации)*; угроза прекращения обслуживания *(например, мобильным оператором при отказе от «смены тарифа»)*; а также необходимость «спасения» денег или иного имущества жертвы, в том числе от... цифровых мошенников.

> При этом следует отграничивать подобные мошеннические инциденты от вымогательства: ложное сообщение о «заражении цифрового устройства жертвы» и требование выплаты за «устранение проблемы», требование денег за отказ от распространения порочащей информации или за устранение реальных программно-технических проблем, причиненных злоумышленником устройству жертвы – являются именно вымогательством.

Характерная черта обоих сценариев — жертва ставится перед необходимостью принятия мгновенного решения, как правило, именно во время коммуникации со злоумышленником, и отказ жертвы не принимается.

В ходе общения жертва «выводится» на программно-технический инструментарий мошенников для непосредственного доступа к деньгам

жертвы, например, фальшивые СМС-коды, фишинговые сайты, страницы-двойники платежных систем, интернет-магазинов и т. п.

профилактика цифрового мошенничества

Как уже было указано, **мошенники в целом эксплуатируют либо стремление жертвы получить легкую дополнительную выгоду, либо страх.** В первом случае наиболее уязвимыми объектами зачастую становятся лица, хоть и обладающие достаточной теоретической финансовой и цифровой грамотностью, но находящиеся в стесненном финансовом положении и потому склонные идти на недостаточно оправданный финансовый риск — в том числе дети, подростки, малообеспеченные, пенсионеры.

Эффективный способ избежать возможного мошенничества – отказ от коммуникации с собеседником с последующей независимой проверкой информации, которую он выдал. А также:

интернет-магазины

1. Оцените отклонение от средне-рыночной цены на товар при помощи поискового сервиса

2. Проверьте время существования интернет-магазина в сети, наличие SSL-сертификата, регистрационные данные и отзывы о работе площадки *(однако в последнем случае стоит помнить о т.н. «накрутках»: обратите внимание на дату создания отзывов – если большинство положительных комментариев появилось за короткий срок, это еще один повод задуматься)*

3. Обратите внимание на отклонение от дизайна, отсутствие обратной связи

4. Соответствует ли домен характеру сайта (например, сайт госоргана расположен не в национальных доменах России .RU и .РФ)? Есть ли ошибки в доменном имени, лишние буквы и символы?

предложения о скидках от имени компаний, банков, мобильных операторов

Самостоятельно свяжитесь с компанией по контактам, найденным на ее официальном сайте. Следует знать, что скидочное предложение, даже если является персональным, может быть подтверждено ее сотрудником

информация, эксплуатирующая страх

Уточните информацию, связавшись с организацией, от имени которой поступило электронное письмо, СМС или телефонный звонок, по контактам, найденным на ее официальном сайте.

Для отдельных вопросов, например штрафов, информацию можно уточнить через интернет-сервисы электронных услуг *(например, «Госуслуги»)*

просьбы и предложения, эксплуатирующие этичность

Если вас уверяют в «ошибочном переводе», предложите мошеннику обратиться к организации, принявшей транзакцию (например, офис мобильного оператора)

В связи с тем, что интернет-мошенничество является преступлением, его жертвам следует обращаться с заявлением о преступлении в правоохранительный орган.

киберунижение

- **Киберунижение** – группа угроз контентного характера, объединяемых целью причинения вреда чести, достоинству и репутации конкретно определяемого человека. Осуществляется на основе персональных данных жертвы, *взятых как из публичного доступа, так и добытых противоправным путем*.

Киберунижение может распространяться и на группу людей, однако эти люди должны быть идентифицируемы на уровне своих основных персональных данных.

К основным формам киберунижения относятся:

Единичные эпизоды оскорблений
при цифровой коммуникации

Троллинг
провоцирующее поведение на цифровой площадке с целью вызвать ответные оскорбления со стороны жертвы и представить последнюю агрессором

Кибербуллинг (кибертравля)
серия оскорблений и клеветнических утверждений в отношении жертвы или группы жертв. Буллинг осуществляется, как правило, на конкретной цифровой площадке или платформе

Киберпреследование (кибersталкинг)
киберунижение, осуществляемое одним и тем же агрессором или группой агрессоров в отношении жертвы на разных интернет-площадках. Характерная черта – переход агрессоров вслед за жертвой на другие платформы, поиск жертвы на новых платформах и возобновление травли на новой площадке

Специфическая форма киберунижения
распространение сцен сексуальной эксплуатации несовершеннолетних, несогласованное распространение информации о сексуальных действиях совершеннолетних лиц (в том числе фото и видео), а также оскорбления и травлю по признакам расы, национальности и религиозной принадлежности, которые принято относить к преступлениям экстремистского характера

Независимо от формы, травля или преследование могут быть:

- **публичными**, то есть осуществляться на публичной платформе, доступной неопределенному количеству пользователей;
- **непубличными**, то есть осуществляться в приватной коммуникации *(в мессенджере, личных сообщениях в соцсетях, электронной почте и т. п.);*
- сочетать публичные и непубличные элементы.

С точки зрения раскрытия персональных данных, киберунижение может осуществляться:

- **без деанонимизации**, то есть в отношении определенного псевдонима;
- **с деанонимизацией,** то есть с открытыми персональными данными жертвы (жертв), включая фото и видео;
- **с фальсификацией персональных данных**, например, с приписыванием псевдониму персональных данных другого человека, использованием так называемых «фотожаб» или дипфейков, публикацией заведомо ложной информации о человеке, порочащей его репутацию.

Киберунижение может быть начато спонтанно, в результате общения на площадке, а может носить запланированный характер. **Мотивом для этого часто становится:**

- реализация неприязненных отношений, возникших в офлайне; продолжение травли, имеющей место в офлайне *(к примеру, из зависти или мести);*
- желание агрессора развлечься или повысить свой социальный статус *(то есть выглядеть «авторитетнее»);*
- месть конкретному человеку, персональные данные и аккаунты которого известны / находятся в открытом доступе;
- «выдавливание» неугодного пользователя с конкретной интернет-площадки.

Часто оскорбления и клевета в процессе киберунижения комбинируются с угрозами, что является одним из самых опасных его элементов. Характер угроз, как правило, зависит от фантазии агрессоров и может варьироваться *(например, угроза заражения устройства жертвы вредоносным ПО, угроза взлома смартфона для доступа к конфиденциальным данным, угрозв физической расправы)*. Перед жертвой в таких случаях встает вопрос оценки степени реальности угрозы, то есть «есть ли смысл на самом деле опасаться высказанных угроз», что выступает дополнительным травмирующим элементом.

Основным фактором, способствовавшим взрывному распространению киберунижения в коммуникационных сервисах, начиная с чатов и заканчивая соцсетями, является одно из главных свойств интернета — **относительная анонимность пользователя**, с точки зрения последнего выглядящая зачастую почти полной.

С психологической точки зрения агрессор почти всегда ощущает себя не только неизвестным, но и недосягаемым — как для жертвы, так и для санкций. Именно это ощущение стимулирует агрессивное поведение даже у тех людей *(особенно детей, подростков и молодежи)*, которые в офлайне предпочитают воздерживаться от него.

Легкость создания аккаунтов от имени другого или вообще несуществующего лица в социальных сетях, при невозможности жертвы его верифицировать, не только способствует киберунижению, но и нередко наводит агрессоров на мысль создания аккаунтов для киберунижения «под чужим флагом» — то есть от имени другого реально существующего человека, в результате чего жертвами становятся как прямой объект киберунижения, так и лицо, якобы от имени которого киберунижение осуществляется.

профилактика киберунижения

Первый этап защиты — **обращение к институтам саморегулирования**, модерационным и администрационным инстанциям *(например, кнопка «Пожаловаться» в социальных сетях).*

Смешанные формы киберунижения, охватываемые УК РФ

Необходимо обращаться в правоохранительные органы

Если в процессе киберунижения фигурируют персональные данные

Формально ведомством, ответственным за безопасность в сфере персональных данных, является Роскомнадзор: ведомство способно выдавать предписания на удаление негативного контента и блокировать ресурс за их неисполнение

Защита от киберпреследования

Эффективный способ — блокировка входящих сообщений от незнакомых контактов. Если киберпреследование перешло в категорию угроз — это является достаточным основанием для обращения в правоохранительные органы

Киберунижение как продолжение неприязненных отношений в офлайне

Поскольку в данном случае киберунижение не является самостоятельным действием, то проблему необходимо решать путем комплексной офлайновой работы с агрессором

Если агрессор является несовершеннолетним, то к такой работе должны привлекаться как родители, так и представители образовательной организации, а возможно и уполномоченные представители правоохранительного органа. Целью такой работы должно быть не только разрешение конфликта, но и формирование у агрессора ощущения неотвратимости наказания за подобное деяние

контентные угрозы террористической и экстремистской направленности

Террористическая и экстремистская активность сочетает в себе публичные и непубличные проявления.

Публичные проявления

- ориентированы на пропаганду соответствующих взглядов, и потому могут встречаться в социальных сетях, на видеохостингах, в публичных каналах мессенджеров
- нередко «маскируются» под исторические, псевдонаучные и иные сообщества соответствующего рода
- создатели подобного контента стараются поддерживать собственную анонимность

Непубличные проявления

- характерна максимальная анонимность
- коммуникация ведется в максимально защищенных мессенджерах со сквозным шифрованием
- используются возможности даркнета — «темного» сегмента интернета с иными протоколами, направленными на повышение конфиденциальности и анонимности

Создатели и адепты подобного контента активно используют два основополагающих свойства интернета: анонимность и трансграничность. Для коммуникации выбираются максимально защищенные от внешнего прочтения инструменты, для хостинга – площадки и юрисдикции (государства) с максимально подходящим законодательством и не сотрудничающие с правоохранительными органами государств, против населения которых направлена террористическая и экстремистская деятельность.

Ключевой момент в определении противоправной сущности подобного контента — его контекст, то есть характер подачи, смысл и цель, которую вкладывает создатель контента при его публикации. Проще говоря, «что он хочет сказать и зачем публикует».

Именно поэтому в правоохранительной деятельности доказательством в подобных делах является комплексная экспертиза, цель которой — установление целей и смыслов публикации.

Формы контента террористической и экстремистской направленности

персонализированные по признаку расы, национальности, религиозной принадлежности оскорбления

специализированная форма киберунижения

Вербовка

в ряды террористических и экстремистских сообществ, исполнителей террористических актов, диверсий, координация деятельности преступных сообществ

Информационные материалы, декларирующие превосходство одной расы, национальности, религии над остальными

могут маскироваться под «историко-патриотические» для соответствующего восприятия новыми целевыми аудиториями

Пропаганда и популяризация насильственных действий террористического и экстремистского характера

цель – устрашение населения со стороны террористических групп

Формирование негативного образа группы лиц по признакам расы, национальности, религиозной принадлежности, возбуждение ненависти и вражды по этим признакам

материалы подобного характера могут состоять из достоверных и верифицируемых фактов – негативный умысел заключается в характере и стратегии подачи, направленной на формирование отрицательного образа соответствующей группы

Призывы к насильственным действиям, а также блокаде, бойкоту, отказу в реализации прав и свобод или ограничению прав и свобод по признаку расы, национальности, религиозной принадлежности, а также иным признакам, в том числе полу, здоровью, политическим убеждениям

подобные действия однозначно являются злоупотреблением правом на свободу слова и самовыражения; их разновидностью могут быть призывы к массовым беспорядкам, депортации, а также взрывам и иным общеопасным действиям

Основной способ профилактики негативного воздействия со стороны подобного контента – развитие у пользователей интернета критического мышления. Критический подход к контенту и изложенным в нем аргументам позволяет избежать «перестройки сознания» и удержаться от романтизирующего воздействия, которое злоумышленники нередко закладывают в свои сообщения.

Беседы о развитии критического мышления необходимы и в том случае, если несовершеннолетний подвержен негативным взглядам «благодаря» психологической обработке в интернете. **Логические контраргументы и наглядные примеры позволяют создать у жертв такого контента иную систему восприятия и заставить критически относиться к искажению фактов или их однобокой подаче, практикуемой злоумышленниками.**

Целесообразно занять время альтернативными делами с позитивным общественным смыслом — они способствуют расширению кругозора, искоренению нетерпимости и развитию товарищеских отношений между представителями разных социальных культур.

В случае оскорблений или угроз, основанных на расовой, национальной или религиозной «подложке», можно не только требовать удаления подобного контента от модераторов сообщества или администрации цифровой площадки, но и обращаться в правоохранительные органы — особенно если есть основания опасаться реальности высказанных угроз. Аналогичные действия могут быть предприняты и в отношении контента/действий с признаками пропаганды террористической или экстремистской идеологии.

пронаркотический контент

Эта категория контента по своим свойствам схожа с террористическим и экстремистским, однако связана с пропагандой и распространением вполне физической, «офлайновой» вещи — наркотических и психотропных веществ.

К особенностям этой угрозы можно отнести следующее:

Контентная активность в интернете тяготеет к закрытым пространствам, поскольку направлена исключительно на получение прибыли от продаж запрещенных веществ

Киберпреступники используют «защищенные» мессенджеры, SIM-карты, зарегистрированные на посторонних лиц

Короткая жизнь сайтов и страниц (всего несколько дней)

При создании подобных ресурсов, применяется максимум средств анонимизации, в том числе фальшивые SIM-карты для регистрации на публичных площадках. Указываемые контакты, как правило, постоянно меняются

Рекрутинговая активность — привлечение через сеть исполнителей, которые могут «доставлять/закладывать продукцию» или обналичивать средства

Как правило, предложения «высокой зарплаты за простейшую работу» ориентированы на подростково-молодежную аудиторию, нуждающуюся в деньгах. Распространяются в соцсетях и каналах мессенджеров, при этом непосредственная коммуникация «работодателя» с «исполнителем» происходит исключительно в мессенджерах со сквозным шифрованием

Опасность подобных объявлений в том, что предлагаемая в них «работа» влечет уголовную ответственность с большим сроком заключения. Для следствия не имеет значения, действовал «курьер» с прямым умыслом или нет (то есть знал или нет, что именно разносит) — значение имеет именно факт «доставки». В связи с чем речь в данном случае идет о втягивании несовершеннолетних и молодежи в преступную деятельность через интернет

профилактика и противодействие

Для профилактики вовлечения несовершеннолетних в преступную деятельность необходима атмосфера высокого доверия внутри семьи. Родители должны быть в курсе коммуникаций подрастающего поколения — это позволяет эффективно защищаться не только от вовлечения в преступную деятельность, включая пронаркотическую, но и от груминга.

- **Груминг** *(англ. grooming — «ухаживание»)* — процесс установления близких отношений с ребёнком или подростком с целью дальнейшей сексуальной эксплуатации; может происходить как в офлайн-пространстве, так и в интернете.

Эффективный способ защиты детей и подростков от вовлечения в потребление наркотиков и преступную деятельность по их распространению — развитие критического и логического мышления. Молодой пользователь должен осознавать всю проблемность потребления подобных веществ, а также риски, которые влечет криминальный заработок в условиях неотвратимости наказания. Это достигается комбинацией усилий школы и семьи, с приоритетом последней, для чего требуется атмосфера доверия, в том числе к компетентности родителей.

На пронаркотическую активность в интернете реагируют администрации как цифровых сервисов, так и большинства мессенджеров. Как правило, задействование мер саморегулирования не составляет проблемы — нередко данная категория уже предусмотрена в форме подачи жалоб. Также возможно обращение в правоохранительный орган.

нарушения в сфере персональных данных

- **Под персональными данными традиционно понимается любая информация, относящаяся к конкретному человеку:** условно, не только паспортные данные, но также его биометрические данные (фотографии и видеоизображения, отпечатки пальцев), биографические сведения и многое другое.

- Отдельная категория — **чувствительные данные *(«специальные категории персональных данных»)*,** компрометация которых способна нанести исключительно серьезный вред человеку, например, информация о состоянии здоровья, политических и общественных взглядах, интимной стороне жизни человека.

- **В понятие «обработка персональных данных», согласно законодательству, входят практически любые действия, совершаемые с персональными данными, за исключением разве что личного хранения их субъектом,** то есть тем лицом, о чьих персональных данных идет речь.

«По умолчанию» режим обработки персональных данных конфиденциальный, однако в некоторых случаях они становятся публичными, например, когда вы размещаете фотографию в соцсетях.

основные характеристики угроз

«Утечка» персональных данных — предоставление доступа к ним неуполномоченному постороннему лицу

Такие данные используются: для подготовки и совершения других злонамеренных действий, в частности цифрового мошенничества и киберунижения; для подготовки преступлений в офлайне, в том числе тяжких и особо тяжких — вплоть до похищений несовершеннолетних

Объединение сведений из нескольких баз позволяет злоумышленникам глубоко раскрыть тайну личной жизни человека и лучше подготовиться, к примеру, к совершению мошеннических действий

Адаптация под актуальные информационные поводы

В качестве ширмы используются фальшивые сайты социологических опросов, анкеты для «получения финансовой помощи» и т.п. Собранная база персональных данных имеет ценность на «черном рынке», плата за которую окупается прибылью от мошеннических действий

Случаи вымогательства, как правило, связаны с чувствительными персональными данными (например, за нераспространение таких данных в публичном пространстве)

В первую очередь это касается интимных изображений, а вывод подобного контента в публичное пространство – форма сильнейшего киберунижения

Фото или видео могут быть похищены непосредственно с устройства жертвы *(программно-техническими средствами, например, подбором пароля)*, однако более частым сценарием является вхождение в доверие к жертве и получение от нее соответствующих изображений добровольно

На текущей стадии развития искусственного интеллекта **могут использоваться также дипфейки с внешностью жертвы**, создание которых облегчается в том случае, если в распоряжении злоумышленника имеется много фотографий или видео жертвы *(которые берутся, как правило, из соцсетей, где жертва их сама опубликовала)*

способы профилактики

Универсальный способ минимизации угроз, связанных с персональными данными — сведение к минимуму их предоставления и обработки. Тщательный анализ возможных последствий от публикации данных также помогает избежать многих компрометирующих последствий.

Да, это возможно не всегда, так как в некоторых случаях предоставление персональных данных предписывается законом.

При этом сам оператор далеко не всегда руководствуется принципами разумности и соразмерности при сборе персональных данных. Чаще всего нарушаются принципы разумности сроков хранения, что и обуславливает высокую уязвимость хранящихся персональных данных.

Но в тех случаях, когда предоставление и хранение персональных данных всецело зависит от субъекта, например, в соцсетях – просто необходимо пойти по пути минимизации.

Крайне осторожно следует относиться и к попыткам сбора персональных данных в интернете, если цель и сроки их обработки остаются непонятными.

Факт распространения интимных фото или видео, а тем более вымогательство таковых, особенно у несовершеннолетних, однозначно является преступлением, а значит поводом для немедленного обращения в правоохранительный орган.

Эффективно реагируют на распространение такого контента и субъекты цифровой индустрии, поэтому можно быть уверенным в прекращении его оборота по поданной в администрацию ресурса жалобе.

При выявлении факта незаконного оборота собственных персональных данных жертва может обратиться в уполномоченный в данной сфере орган, которым является Роскомнадзор, или в прокуратуру как вневедомственный надзорный орган, обладающий несколько большими полномочиями.

Следует помнить, что информационный вред относится к числу невосполнимых: единожды скомпрометированные данные остаются таковыми навсегда, особенно это касается биометрических данных, которые не могут быть заменены в принципе. Поэтому весьма эффективным является путь профилактики, то есть максимального отказа от выпуска в оборот своих персональных данных — особенно чувствительных, интимных и биометрических.

Вдумчивая «собственная политика» публикаций в интернете также станет определенным гарантом от возможных инцидентов.