СЕРИЯ

КАК ВЫЖИТЬ В ЭКСТРЕМАЛЬНЫХ УСЛОВИЯХ

ОБЩЕСТВО ЗА БЕЗОПАСНОСТЬ

Ресурсный центр добровольчества в сфере ЧС

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

ОГЛАВЛЕНИЕ

ЦИФРОВАЯ ЭРА: ЭВОЛЮЦИЯ ТЕХН КОТОРЫЙ МЫ СО

В непрерывном пульсе современной жизни, мир преобразуется под влиянием вихря цифровых инноваций, предоставляя нам удивительные возможности и вызовы. От первых древних средств для учета и расчетов до современных умных технологий и Интернета вещей, каждый этап нашей технологической эволюции оставляет свой след в облике нашей цифровой среды.

Телекоммуникационные технологии стали катализатором социальных и культурных трансформаций, сближая людей на разных концах земли и создавая невидимые, но мощные связи в нашей повседневной жизни.

Информационные технологии (ИТ) являются основой современного цифрового мира, и их эволюция с середины XX века продолжает волновать наш образ жизни, предоставляя нам невероятные возможности и переосмысленные ценности.

Информационно-коммуникационные технологии (ИКТ) представляют собой мощный инструмент обмена информа-

ОЛОГИЙ И МИР, ЗДАЕМ

цией и взаимодействия в нашем современном обществе. С их появлением на свет, мы вступили в новую эпоху связности и обмена данными.

Мультимедийные технологии представляют собой интеграцию различных форм контента, включая изображения, звук и видео. Их появление в конце XX века стало важным этапом в развитии технологий, привнося в нашу жизнь новые способы восприятия и общения.

Виртуальные технологии открывают перед нами возможности погружения в виртуальные миры и взаимодействия с ними. С их появлением, мы стали свидетелями удивительных изменений в том, как мы воспринимаем и взаимодействуем с окружающим миром.

Цифровые технологии стали ключевым элементом современного общества, переформировав способы взаимодействия и восприятия мира. Их влияние ощущается повсюду, от нашего дома до рабочего места, и их появление привнесло несравненные уровни эффективности и удобства в нашу повседневную жизнь.

1.1. ЦИФРОВЫЕ ТЕХНОЛОГИИ

В цифровых технологиях данные играют ключевую роль, представляя основной строительный материал для функционирования и развития систем. Они представляют информацию в цифровой форме, то есть в виде чисел и символов, что обеспечивает их легкость обработки и передачи. В современном цифровом мире огромное количество данных создается и накапливается каждый день. Эта информация становится ценным ресурсом для принятия решений, и анализ данных становится важным инструментом для выявления закономерностей, трендов и возможностей, что способствует более эффективному функционированию технологий и обеспечивает прогресс в различных областях, включая бизнес, науку и общество в целом.

Цифровая среда представляет собой комплекс условий и возможностей, в котором человек взаимодействует с цифровыми технологиями и информационно-коммуникационной инфраструктурой. Она создает окружение, в котором люди имеют доступ к различным цифровым ресурсам и инструментам, предоставляя возможности для самореализации, личностно-профессионального развития, а также решения разнообразных бытовых и профессиональных задач.

Цифровая среда включает в себя широкий спектр элементов, таких как интернет, мобильные устройства, программное обеспечение, социальные сети, облачные сервисы и другие технологии. Эти компоненты создают основу для взаимодействия человека с цифровым миром, предоставляя ему доступ к информации, коммуникации, образованию, развлечениям и другим сферам жизни.

Цифровая среда не только обеспечивает удобство и эффективность в повседневной жизни, но также открывает новые возможности для обучения, творчества, предпринимательства и са-

мореализации. Люди могут использовать цифровые технологии для расширения своих знаний, создания контента, установления связей с другими людьми и достижения профессиональных целей.

В целом, цифровая среда стала неотъемлемой частью современного общества, формируя новый контекст для жизни и деятельности людей, а также оказывая влияние на их образ мышления, общение и взаимодействие с окружающим миром.

1.2. ЦИФРОВЫЕ ЦЕННОСТИ

С ускоренным развитием цифровых технологий наш образ жизни претерпел значительные изменения, и с этими изменениями пришли новые, цифровые аналоги традиционных ценностей. Вместо обычных источников информации теперь цифровые ресурсы стали неотъемлемой частью нашей повседневной жизни,

предоставляя доступ к огромному объему данных и знаний.

Деньги в бумажной форме и чеки уступают место цифровым финансовым инструментам, таким как электронные кошельки и онлайн-платежи, предоставляя удобные и безопасные способы управления финансами.

Традиционные формы связи, такие как письма и личные встречи, уступают место цифровым каналам общения. Социальные сети, мессенджеры и видеозвонки позволяют поддерживать связь с людьми в режиме реального времени, независимо от географического расположения.

В сфере образования бумажные учебники и материалы уступают место цифровым образовательным ресурсам, таким как онлайн-курсы и электронные учебники, предоставляя более гибкие и доступные возможности обучения.

Традиционные развлечения, такие как кинотеатры и музеи, теперь дополняются цифровыми развлечениями, такими как стриминговые сервисы и онлайн-игры, предоставляя новые формы отдыха и развлечений.

Здравоохранение также претерпевает изменения, где бумажные медицинские карты заменяются цифровыми системами здравоохранения и телемедициной, предоставляя более удобные и эффективные способы ухода за здоровьем.

Туристические карты и агентства уступают место цифровым навигационным приложениям и онлайн-бронированию путешествий, предоставляя более гибкие и персонализированные варианты путешествий.

Документы в бумажной форме и офисные встречи сменяются электронными документами, удаленной работой и виртуальными конференциями, создавая новые подходы к работе и деловым взаимодействиям.

Вместе с этим развитием цифровых технологий появились цифровые активы, доступ к которым может стать объектом киберугроз. Среди цифровых активов, являющихся важными для обычного человека, следует выделить:

1. Финансовые данные:

• Электронные банковские счета и кошельки.

• Электронные деньги и криптовалютные кошельки.

• Программы лояльности и бонусные балы, которые можно использовать для оплаты.

• Инвестиционные портфели и цифровые акции.

• Электронные копии финансовых отчетов и документов.

2. Персональные данные:

• фамилия, имя, отчество;

• место, дата рождения;

• место постоянной или временной регистрации;

• фотография или видеозапись человека, позволяющие идентифицировать человека;

• сведения о детях, родственниках, семейном положении;

• сведения о заработной плате;

• оценка навыков, личностных качеств;

• индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);

• информация о судимостях, или их отсутствии;

• номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;

• паспортные данные, СНИЛС, ИНН;

• Биометрические данные (отпечатки пальцев, сканы лица).

3. Здравоохранение и медицинская информация:

• Электронные медицинские карты и истории болезней.

• Результаты анализов и обследований.

• Информация о лекарствах и лечении.

4. Цифровые ключи и пароли:

• Электронные пароли для входа в аккаунты (электронная почта, социальные сети, онлайн-магазины, торговые площадки и маркетплейсы, онлайн-банкинг т.п.).

• Электронные ключи и ключи шифрования для защиты файлов и данных.

• Коды двухфакторной аутентификации.

• Электронные ключи доступа к зданиям или транспорту.

• Идентификационные карты и браслеты с RFID-чипами.

5. Цифровой контент и интеллектуальная собственность:

• Цифровые художественные работы (графика, иллюстрации).

• Электронные музыкальные композиции и аудиозаписи.

• Цифровые фотографии и видеоконтент.

• Лицензии на программное обеспечение и приложения.

• Электронные книги и учебные материалы.

• Электронные копии научных публикаций и статей.

• Цифровые проекты и исследования.

6. Личные данные в социальных сетях:

• Личные профили в социальных медиа.

• Переписка и личные сообщения.

• Фотографии и видео, размещенные в социальных сетях.

7. Данные, связанные с образованием:

• Электронные сертификаты и дипломы об образовании.

• Цифровые записи учебных достижений.

• Электронные портфолио студентов и профессионалов.

8. Электронные билеты и абонементы:

• Цифровые билеты на мероприятия и концерты.

• Электронные абонементы на услуги и развлечения.

• Цифровые билеты на транспортные средства и перевозки.

9. Данные, связанные с профессиональной деятельностью:

• Цифровые версии и копии договоров и соглашений.
• Цифровые копии бизнес-планов и стратегий.
• Информация о клиентах и контрагентах.
• Электронные подписи и согласования.

10. Информация об онлайн-активности, цифровые следы и метаданные:

• Геолокационные данные от устройств.
• Метаданные фотографий и файлов.
• История использования устройств и приложений.
• Персональные настройки в приложениях и устройствах.
• История интересов и предпочтений в онлайн-сервисах.
• История поисковых запросов.
• Информация о посещенных веб-сайтах.
• Данные об онлайн-покупках и транзакциях.

С учетом значимости этих цифровых активов для личной жизни и безопасности, обеспечение их защиты и безопасности становится критически важным в контексте растущих угроз кибербезопасности. Индивидуальная осведомленность, применение сильных методов аутентификации и регулярное обновление мер безопасности становятся ключевыми аспектами для предотвращения утраты или несанкционированного доступа к цифровым активам.

1.3. ЦИФРОВОЙ СЛЕД И ЦИФРОВОЙ ПРОФИЛЬ

Цифровой след - совокупность данных, которые пользователь генерирует во время пребывания в цифровой среде. Цифровой след представляет собой своеобразный «цифровой отпечаток» жизни и личности человека, отражающий его интересы, потребности, социальный и интеллектуальный уровень развития, а так-

же культурный уровень и психологические особенности. Цифровой след можно разделить на два вида:

1. Активный цифровой след (данные, оставленные пользователем намеренно или по незнанию), например:

• Социальные медиа-публикации: Пользователь размещает свои фотографии, статусы, комментарии, выражая свои мысли и эмоции.

• Онлайн-покупки: Введение личных данных при совершении покупок в интернете, оставляя след о своих предпочтениях и потребительском поведении.

• Блоги и статьи: Публикация собственных статей, заметок или блогов, представляя свои идеи и экспертное мнение.

2. Пассивный цифровой след (данные, оставленные пользователем непроизвольно), например:

• История поисковых запросов: Автоматическое сохранение запросов, совершаемых в поисковых системах, отражает интересы и информационные потребности пользователя.

• Геолокационные данные: Автоматическое сохранение местоположения при использовании мобильного устройства или фотографировании, что формирует карту перемещений пользователя.

• Куки и отслеживание веб-сайтов: Автоматическое сбор данных о посещенных веб-сайтах, предпочтениях и поведенческих особенностях в процессе интернет-серфинга.

Оба типа цифрового следа формируют полную картину онлайн-присутствия пользователя, предоставляя информацию о его предпочтениях, активностях и поведенческих тенденциях.

Цифровой профиль - это собранный и организованный набор данных о человеке, полученный из его цифрового следа. Этот профиль может включать в себя различные аспекты онлайн-при-

сутствия и активности.

Вот некоторые ключевые элементы цифрового профиля, которые могут быть созданы на основе цифрового следа:

• Социальные медиа-профили: Включают в себя информацию о пользователях в социальных сетях, такую как личные данные, публикации, фотографии, группы, в которых они состоят, и взаимодействие с другими пользователями.

• История поисковых запросов: Список запросов, выполненных пользователем в поисковых системах, может дать представление о его интересах, потребностях и предпочтениях.

•Онлайн-активность: Информация о посещенных веб-сайтах, онлайн-покупках, совершенных транзакциях и других действиях в цифровом пространстве.

• Местоположение: Данные о том, где и когда пользователь находился в определенное время, основанные на геотегах в фотографиях, чек-инах в социальных сетях и использовании GPS.

• Контент: Загруженные фотографии, видео, аудио и другие медиафайлы.

• Электронная почта: Коммуникация через электронную почту, включая отправленные и полученные сообщения.

• Онлайн-репутация: Отзывы, комментарии и рейтинги, оставленные другими пользователями, могут также влиять на цифровой профиль.

Создание цифрового профиля может быть как следствием активной деятельности пользователя, так и автоматическим процессом сбора данных со стороны платформ и сервисов. Цифровой профиль может оказать влияние на различные аспекты жизни человека, как в онлайн-среде, так и в реальной жизни. Вот некоторые из возможных воздействий цифрового профиля:

1. Онлайн-репутация: Цифровой профиль является важным элементом формирования онлайн-репутации. Отзывы, комментарии и другие элементы цифрового следа могут сказываться на том, как вас видят другие в онлайн-среде.

2. Карьера: Работодатели могут использовать цифровые профили в процессе рекрутинга для оценки личности, профессиональных навыков и репутации потенциального сотрудника.

3. Безопасность и конфиденциальность: Недостаточно защищенный цифровой профиль может привести к утечкам личной информации, что может быть использовано в киберпреступлениях или для мошенничества.

4. Реклама и персонализация: Основываясь на данных цифрового профиля, компании могут настраивать рекламу и предлагать персонализированный контент.

5. Социальные взаимодействия: Цифровой профиль влияет на взаимодействия с другими пользователями в социальных сетях и других онлайн-платформах.

6. Кредитная история: Некоторые сервисы и компании могут использовать данные из цифрового профиля при оценке кредитоспособности.

7. Поведенческая аналитика: Большие данные и аналитика могут использоваться для прогнозирования поведенческих тенденций и предоставления персонализированных рекомендаций.

8. Доступ к сервисам: Некоторые онлайн-сервисы и платформы могут предоставлять или ограничивать доступ на основе данных из цифрового профиля.

Чтобы управлять своим цифровым профилем, важно осознанно управлять своим цифровым следом и использовать настройки конфиденциальности, чтобы контролировать доступ к своей личной информации. Приведем примеры действий, которые направленны на самостоятельное формирование вашего цифрового профиля:

1. Измените настройки в социальных сетях:

Регулируйте настройки конфиденциальности в социальных сетях и других онлайн-платформах, чтобы контролировать, кто видит вашу личную информацию. Ограничьте доступ к личным данным только тем, кого вы знаете и кому доверяете.

2. Следите за тем, что вы размещаете в сети:

Будьте внимательными при размещении личной информации онлайн. Предвидьте, какие могут быть последствия публикаций. Избегайте разглашения слишком многих деталей о личной жизни. Избегайте оскорбительных или спорных высказываний, которые могут негативно сказаться на вашей репутации.

3. Поддерживайте безопасность аккаунтов:

Используйте сильные пароли и двухфакторную аутентификацию для защиты своих онлайн-аккаунтов. Периодически меняйте пароли.

4. Управляете отслеживанием:

Определите настройки отслеживания в браузере и управляйте файлами кук для контроля за тем, какие данные хранятся о вас. Используйте VPN для шифрования интернет-соединения и анонимизации вашего онлайн-присутствия.

5. Регулярно анализируйте ваш цифровой след:

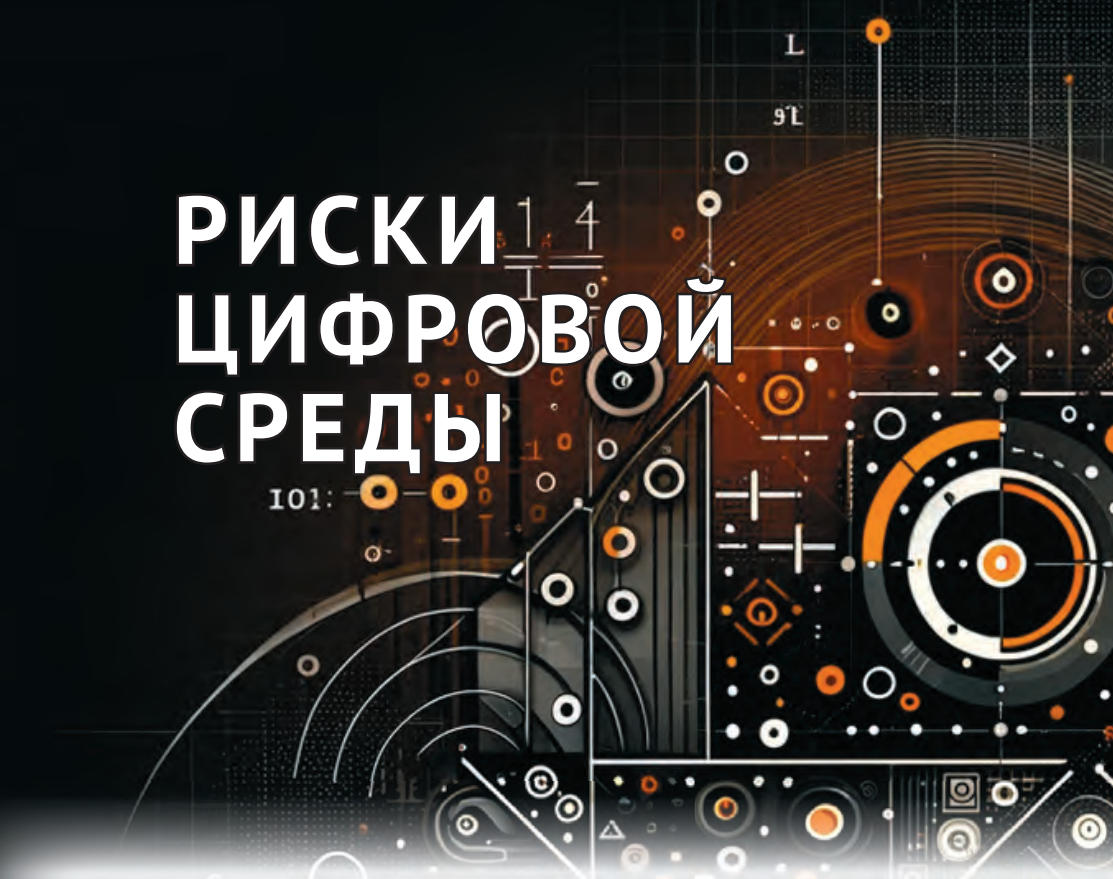
Периодически проверяйте свой цифровой след, чтобы убедиться, что он соответствует вашим предпочтениям и целям.

6. Удаляйте ненужную информацию:

Удаляйте устаревшие или ненужные аккаунты и информацию. Постоянно оценивайте и удаляйте ненужные посты, фотографии или другие данные, которые могут привести к нежелательным последствиям.

Принятие этих мер поможет вам контролировать свой цифровой след и минимизировать потенциальные риски, связанные с использованием онлайн-платформ.

РИСКИ ЦИФРОВОЙ СРЕДЫ



В современном мире, где цифровая среда становится неотъемлемой частью повседневной жизни, взаимосвязь между деятельностью человека и цифровым пространством становится все более тесной и влияет на различные аспекты нашего существования. От социальных сетей и онлайн-покупок до поисковых запросов и электронной переписки, цифровой след каждого человека становится уни-

кальным отражением его интересов, предпочтений и поведенческих особенностей. Однако эта интенсивная взаимосвязь также вносит свой вклад в появление различных рисков, связанных с конфиденциальностью, безопасностью и формированием онлайн-репутации.

Как в любой среде, в цифровой среде есть риски и опасности, которые можно разделить на пять больших групп:

1. Технические риски, которые связывают с незаконным доступом, повреждением программного обеспечения компьютера или хранящейся на нем информации, нарушением конфиденциальности или хищением цифровых активов.

2. Потребительские риски, возникающие в результате злоупотребления правами потребителя или его обмана.

3. Контентные риски, возникающие в процессе использования находящихся в Интернете материалов

4. Коммуникационные риски, возникающие в процессе общения и межличностного взаимодействия пользователей в Интернете.

5. Риски интернет-зависимости, связанные с возникновением непреодолимой тяги и чрезмерному использованию социальных сетей, видеоигр, цифрового контента и устройств.

Важно отметить, что риски в цифровой среде и риски в повседневной жизни во многом схожи, и нужно учиться видеть эти риски, предупреждать их возникновение и устранять последствия.

2.1. ТЕХНИЧЕСКИЕ РИСКИ

Технические риски представляют собой потенциальные угрозы, связанные с техническими аспектами информационных систем. Они могут возникнуть из-за недостатков в программном обеспечении, аппаратных средствах, сетевой инфраструктуре и других технических компонентах. Проявление технических рисков может привести к различным последствиям, таким как потеря данных, нарушение конфиденциальности, повреждение системы и другие.

Примеры проявления технических рисков:

• Повреждение программного обеспечения компьютера: атака вирусом или вредоносным ПО, которые могут повредить операционную систему или приложения.

• Повреждение хранящейся информации: атака на базы данных с целью уничтожения, изменения или блокировки данных.

• Хищение персональной информации: кража личных данных с помощью вредоносных программ или техник социальной инженерии.

• Использование вычислительных ресурсов: атаки на вычислительные ресурсы с целью использования их для майнинга криптовалюты или запуска распределенных атак.

Угрозы технических рисков:

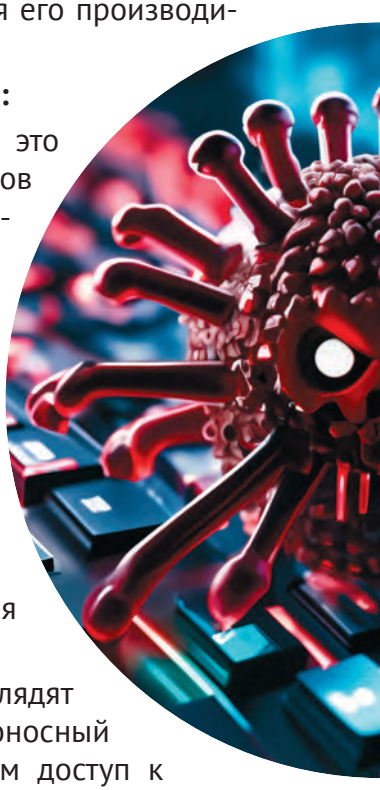
• Вредоносное программное обеспечение. Зловредные программы, такие как вирусы, троянские кони, шпионское ПО.

• Атаки на пароли. Попытки взлома паролей с использованием методов брутфорса, словарных атак или социальной инженерии.

• Фишинг. Отправка ложных электронных писем с целью обмана пользователей и получения их личной информации.

• Спам. Рассылка нежелательных сообщений, которые могут содержать вирусы или ссылки на вредоносные ресурсы.

• Атаки на отказ в обслуживании. Массовые запросы к серверу с целью перегрузки его ресурсов и снижения его производительности.



1. Вредоносное программное обеспечение:

Вредоносное программное обеспечение это обобщенное название для различных видов вредоносных программ, которые предназначены для нанесения вреда компьютерной системе, пользователям или сетям. Перечислим основные виды вредоносных программ с которыми сталкиваются пользователи:

• Компьютерные вирусы: программы, разработанные для внедрения в компьютерные системы и вызывания различных негативных эффектов. Они могут прикрепляться к исполняемым файлам, встраиваться в системные компоненты или распространяться через сеть.

• Троянские кони: Программы, которые выглядят как полезные, но при этом скрывают вредоносный функционал, предоставляя злоумышленникам доступ к системе.

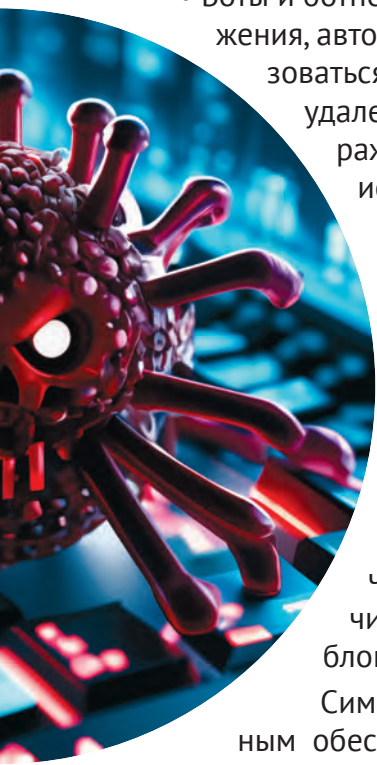
• Шпионское программное обеспечение: Программы, собирающие информацию о пользователях без их согласия с целью незаконного использования.

• Рекламное программное обеспечение: Программы, отображающие навязчивую рекламу, часто собирающие информацию о пользовательском поведении.

• Программное обеспечение, нацеленное на вымогательство: Вредоносные программы, блокирующие доступ к данным или

устройству до тех пор, пока не будет уплачен выкуп.

• Интернет-черви: Самостоятельно распространяющиеся по компьютерным сетям программы, использующие ошибки в программном коде и уязвимости операционной системы для проникновения на устройства пользователей.



• Боты и ботнеты: представляют собой программные приложения, автоматизирующие задачи в сети, и могут использоваться для подчинения устройств пользователя удаленному контролю хакера. Ботнет - это сеть зараженных ботами устройств, которые могут быть использованы для массовых атак, отправки спама, проведения кибератак и других вредоносных действий.

• Вирусы-майнеры, также известные как криптовалютные майнеры: представляют собой вид вредоносных программ, которые используют вычислительные ресурсы зараженного компьютера для майнинга криптовалюты. Эти программы злоупотребляют вычислительной мощностью целевой системы, чтобы решать сложные математические задачи, необходимые для создания новых блоков в блокчейне криптовалюты.

Симптомы заражения вредоносным программным обеспечением могут существенно различаться в зависимости от конкретного типа вредоносной программы. Вот общий список симптомов, на которые стоит обратить внимание при подозрении на заражение:

• Снижение производительности: замедление работы компьютера, задержки при открытии файлов или запуске программ.

• Необъяснимое использование ресурсов: повышенное использование процессора, оперативной памяти или сетевого трафика без видимых причин.

• Изменения в работе приложений: необычное поведение

программ, их зависание или аварийное завершение работы.

• Частые сбои и перезагрузки: необъяснимые сбои операционной системы или перезагрузки компьютера.

• Появление рекламы: всплывающие окна, баннеры, рекламные вставки на веб-сайтах, которые ранее не отображались.

• Изменения в браузере: изменение стартовой страницы, поискового движка или домашней страницы без вашего разрешения.

• Новые расширения и плагины: появление новых расширений или плагинов в вашем браузере, которые вы не устанавливали.

• Проблемы с запуском антивирусных средств: отключение антивирусного программного обеспечения или других средств безопасности без вашего согласия.

• Отключение автоматических обновлений операционной системы или антивирусного программного обеспечения.

• Неожиданные изменение настроек системы, запуск новых служб, или изменения в системных файлах.

• Загрузка неизвестных программ, автоматическая загрузка программ или файлов без вашего согласия. Обнаружение новых программ или сервисов в списке установленного программного обеспечения, которые вы не устанавливали.

• Появление новых иконок на рабочем столе: появление новых ярлыков или иконок на рабочем столе, которые вы не устанавливали.

• Заблокированный доступ к файлам: неожиданные проблемы с доступом к файлам, блокировка или шифрование данных (часто характерно для вирусов-вымогателей).

• Отправка спама из вашего аккаунта: уведомления от провайдера интернета о подозрительной активности, такой как отправка спама из вашего аккаунта. Отправка подозрительных сообщений от вашего имени вашим контактам в электронной почте, социальных сетях или мессенджерах.

Если вы замечаете хотя бы несколько из этих признаков, ре-

комендуется провести тщательную проверку системы с использованием антивирусного программного обеспечения и других средств безопасности.

Как обезопасить себя от вредоносного программного обеспечения:

• Используйте антивирусное программное обеспечение: регулярно обновляйте и сканируйте систему.

• Используйте Брандмауэр (Фаервол) —средство безопасности, которое служит для защиты компьютерных сетей от несанкционированного доступа и контроля сетевого трафика.

• Обновляйте программное обеспечение: включая операционную систему, браузеры и другие приложения.

• Будьте осторожны в интернете: избегайте сомнительных веб-сайтов и не открывайте подозрительные вложения.

• Резервное копирование данных: регулярно создавайте резервные копии важных данных и храните их в надежном месте.

• Не используйте административные права без надобности: используйте учетную запись с минимальными привилегиями для повседневных задач.

Что делать, если стали жертвой вредоносного программного обеспечения:

1. Изолируйте устройство: Отключите его от сети, чтобы предотвратить распространение вредоносного ПО.

2. Сканируйте систему: Используйте антивирусное программное обеспечение для поиска и удаления вредоносных программ.

3. Измените пароли: Если была скомпрометирована личная информация, измените пароли.

4. Обратитесь за помощью: В случае вымогательства или серьезного инцидента, обратитесь за помощью к профессионалам в области кибербезопасности или правоохранительным органам. 2. Атаки на пароли

Атаки на пароли представляют серьезную угрозу для безопасности информации. Злоумышленники могут использовать различные методы для подбора или обхода паролей, пытаясь получить несанкционированный доступ к учетным записям. Такие атаки могут быть направлены на различные системы, включая учетные записи пользователей, файлы с паролями или коды доступа к зашифрованным данным.

Одним из распространенных методов атаки на пароли является «брутфорс» (от англ. brute force — грубая сила), при котором злоумышленник систематически и последовательно пытается все возможные комбинации символов (пароли), чтобы найти правильный. Эта атака основывается на том, что, не зная пароль заранее, злоумышленник может перебрать все возможные комбинации в надежде найти ту, которая действует. Такой процесс может занять очень много времени, и один из способов его сократить — использовать для атаки словари. Программы для брутфорса могут использоваться для автоматизации этого процесса, что позволяет атакующим быстро проверять тысячи, миллионы или даже миллиарды возможных паролей.

Для защиты от атак на пароли рекомендуется принимать следующие меры:

1. Используйте сложные пароли

Создавайте пароли, которые сложно подобрать. Существуют

несколько методов, которые помогут вам удовлетворить требования безопасности, сохраняя при этом доступность:

• Используйте Фразу или Словосочетание: Выберите фразу, предложение или словосочетание, которое имеет для вас особенное значение. Например, «Летом2023НаМоре».

• Смешивание Регистра: Используйте комбинацию заглавных и строчных букв. Это может быть, например, первая буква каждого слова в вашей фразе.

• Добавьте Цифры и Спецсимволы: Вставьте цифры и спецсимволы в середину или конец пароля. Например, «Летом2023@НаМоре».

• Сокращенные Слова: Используйте сокращенные формы слов, но добавьте к ним цифры и спецсимволы. Например, «P@ssw0rd!».

• Акронимы: Создайте пароль, используя первые буквы слов во фразе или предложении. Например, «ЯЛюблюЛето2023!» становится «ЯЛЛ2023!».

• Используйте Акценты и Орфографические Ошибки: Внесите в пароль акценты или создайте орфографические ошибки. Например, «Котэ123!».

• Создайте аббревиатуру из слов предложения: Возьмите первую букву каждого слова из какого-то предложения. Например, «Сегодня Хороший День Для Прогулки» станет «СХДДП».

• Используйте особенные даты: Используйте цифры, связанные с важными для вас датами, и добавьте их к паролю.

2. Регулярно меняйте пароли

Обновляйте свои пароли периодически, даже если нет подозрений на компрометацию. Это может предотвратить несанкционированный доступ в случае утечки данных.

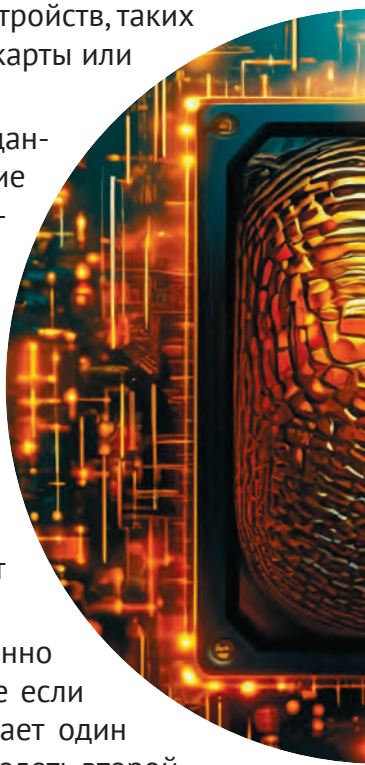
3. Используйте Двухфакторную Аутентификацию

Двухфакторная аутентификация (2FA) — это метод обеспечения безопасности, который требует предоставления двух различных форм идентификации для подтверждения личности

пользователя. Этот подход повышает уровень безопасности по сравнению с обычным вводом логина и пароля. При двухфакторной аутентификации используются два из следующих факторов:

• Что-то, что вы знаете (Как пароль): Это может быть стандартный логин и пароль, который пользователь вводит для доступа к учетной записи.

• Что-то, что у вас есть (Как физическое устройство): Это может включать в себя использование физических устройств, таких как мобильные устройства, USB-ключи, смарт-карты или токены.



• Что-то, что вы являетесь (Биометрические данные): Это может включать в себя биометрические данные, такие как отпечатки пальцев, сканирование сетчатки глаза или распознавание лица.

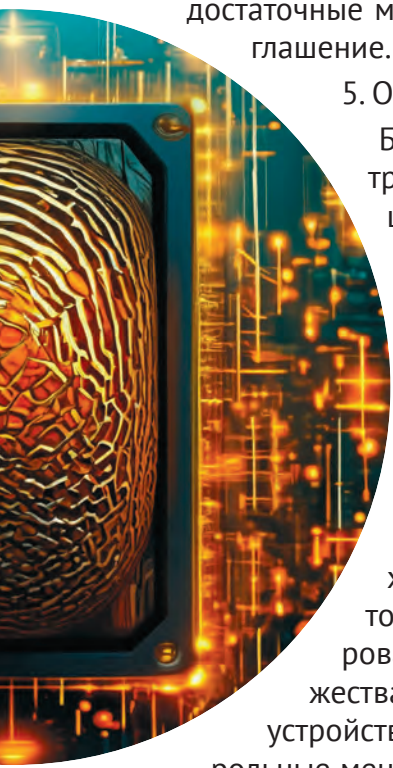
Для успешной аутентификации пользователь должен предоставить два из этих факторов. Например, после ввода логина и пароля (что пользователь знает), система может отправить одноразовый код на мобильное устройство пользователя (что у пользователя есть). Этот код, который действителен только в течение короткого времени, предоставляет второй уровень проверки.

Двухфакторная аутентификация существенно повышает уровень безопасности, так как даже если злоумышленник узнает или поддельно получает один из факторов, ему все равно нужно будет преодолеть второй, что затрудняет успешные попытки несанкционированного доступа. Этот метод особенно важен для защиты учетных записей в банковских системах, электронной почте, онлайн-сервисах и других системах, где конфиденциальность данных играет критическую роль.

4. Избегайте использования одинаковых паролей на разных сайтах:

Не используйте один и тот же пароль для нескольких учетных записей. В случае утечки одного пароля, другие аккаунты останутся защищенными.

Утечки паролей — это ситуации, когда информация о паролях пользователей становится доступной несанкционированным лицам или организациям. Это может произойти из-за различных причин, таких как взлом баз данных, кража учетных записей, недостаточные меры безопасности или даже случайное разглашение.



5. Остерегайтесь Фишинга

Будьте внимательны к подозрительным электронным письмам или веб-сайтам, предлагающим ввести ваш пароль. Проверяйте адреса электронных писем и URL-адреса, прежде чем предоставлять личную информацию.

6. Используйте Парольные Менеджеры

Парольный менеджер — это специализированное программное или аппаратное средство, предназначенное для безопасного и удобного управления учетными данными пользователей. Он обеспечивает хранение и генерацию сложных паролей, автоматическое заполнение полей ввода, шифрование сохраненных данных, поддержку множества учетных записей, синхронизацию между устройствами, а также советы по безопасности. Парольные менеджеры позволяют пользователям создавать уникальные пароли для каждого онлайн-сервиса, что повышает уровень безопасности и облегчает процесс управления доступом к различным аккаунтам..

7. Проверка и профилактика

Регулярно проверяйте активность своих учетных записей. Если замечены подозрительные действия, немедленно измените пароли и предпримите соответствующие меры.

ФИШИНГ

Фишинг (от англ. «fishing» – рыбалка) — это вид кибератак, при котором злоумышленники пытаются обмануть людей, выдавая себя за надежные источники, чтобы получить конфиденциальные данные, такие как логины, пароли, данные кредитных карт или другую чувствительную информацию. Атаки фишинга могут проявляться различными способами, но обычно включают манипуляции с социальной инженерией и подделку легитимных коммуникаций.

Примеры проявления фишинга:

• Фишинговые Электронные Письма: Злоумышленники могут отправлять электронные письма, выглядящие как официальные уведомления от банков, интернет-провайдеров или других организаций, с просьбой ввести личные данные на поддельных веб-сайтах.

• Фишинговые Сайты: Создание поддельных веб-сайтов, которые могут быть практически неотличимы от легитимных, с целью выманивания логинов и паролей.

• Телефонные Атаки: Злоумышленники могут представляться службой поддержки или другими доверенными организациями, пытаясь убедить жертву предоставить свои личные данные по телефону.

• Сообщения в Социальных Сетях: Злоумышленники могут использовать социальные сети для отправки фишинговых сообщений, представляясь друзьями, коллегами или официальными аккаунтами.

Ниже перечислены некоторые характерные признаки фишинговых электронных писем:

• Адрес отправителя: проверьте адрес отправителя. Фишин-

говые письма могут приходить от адресов, которые кажутся похожими на официальные, но имеют небольшие отличия или использование свободных почтовых служб.

• Орфографические и грамматические ошибки: фишинговые письма часто содержат ошибки в правописании и грамматике. Официальные сообщения обычно проходят проверку на предмет таких ошибок.

• Требование срочных действий: мошеннические сообщения часто пытаются создать срочную ситуацию, требуя мгновенных действий, чтобы склонить вас к предоставлению личной информации без должного размышления.

• Отсутствие персонализации: некоторые фишинговые письма могут быть отправлены массово и содержать общие обращения, например «Уважаемый клиент», вместо ваших фамилии и имени.

• Ссылки и вложения: будьте осторожны с ссылками и вложениями. Наведите курсор на ссылку, чтобы посмотреть ее адрес, но не кликайте. Фишинговые сайты могут быть подделаны, а вложения могут содержать вредоносный код. Не скачивайте и не открывайте приложения из электронных писем, особенно если они пришли от незнакомых источников.

• Несовпадение адресов ссылок: проверьте, соответствуют ли адреса ссылок фактическим доменам организации. Фишинговые письма могут использовать поддельные домены, которые напоминают официальные.

• Необычные запросы информации: фишинговые письма могут запрашивать необычные или конфиденциальные данные, такие как пароли, номера кредитных карт или счета для перевода денег, которые не должны быть предоставлены в переписке.

Осмотрительность и внимание к деталям помогут вам избежать попадания в схемы фишинга и обеспечат большую безопасность вашим личным данным.

СПАМ

Спам — это нежелательные, массовые сообщения, которые отправляются через электронную почту, текстовые сообщения, социальные сети или другие коммуникационные каналы с целью рекламы, маркетинга или распространения вредоносного контента. Проявления спама разнообразны, и включают в себя несанкционированную почту, рекламные сообщения и сообщения с вирусами.

Примеры проявлений спама:

Электронная Почта (Email): Нежелательные письма, предложения и рекламные сообщения, часто с содержанием вредоносных вложений или ссылок.

Текстовые Сообщения (SMS): Массовые текстовые сообщения с предложениями о продаже товаров, услуг или поддельными уведомлениями.

Социальные Сети: Автоматизированные боты могут распространять спам в комментариях, личных сообщениях или публикациях.

Форумы и комментарии на сайтах: Нежелательные сообщения и реклама на форумах или в комментариях к статьям.

Автоматические Телефонные Звонки: Автоматические телефонные звонки с рекламой, опросами или мошенническими предложениями.

Опасности, связанные со спамом:

Распространение Мошенничества: Спам может содержать мошеннические предложения, вредоносные вложения или ссылки на поддельные веб-сайты.

Потеря Времени и Ресурсов: Пользователи тратят время на фильтрацию и удаление спама, а также могут терять ресурсы на борьбу с вредоносными последствиями спама.

Похищение Личной Информации: Спам может быть использован для сбора личной информации через фишинговые атаки.

Как обезопасить себя от спама:

Используйте Антиспамовые Фильтры: Антиспамовые фильтры в почтовых клиентах и других коммуникационных приложениях помогают фильтровать нежелательные сообщения.

Не Раскрывайте Личные Данные: Будьте осторожны при предоставлении личных данных в ответ на спамовые запросы.

Не Открывайте Сомнительные Вложения и Ссылки: Не открывайте вложения и не переходите по ссылкам в сообщениях от незнакомых отправителей.

Настройте Приватность в Социальных Сетях: Ограничьте видимость ваших профилей и настройте фильтры приватности в социальных сетях.

Что делать, если стали жертвой спама:

Не отвечайте на подозрительные сообщения, так как это мо-

жет подтвердить вашу активность мошенникам.

Блокируйте отправителя и используйте функции жалобы в приложениях, чтобы предотвратить получение дальнейшего спама от них.

Используйте инструменты для борьбы со спамом в вашем почтовом клиенте или мессенджере.

Основные способы защиты

Основные способы защиты от технических рисков включают в себя:

Использование антивирусного программного обеспечения:

Установка эффективного антивирусного программного обеспечения помогает выявлять и удалять вредоносные программы, троянские кони, шпионские программы и другие угрозы.

Настройка Файервола:

Файерволы могут блокировать нежелательный сетевой трафик и предотвращать несанкционированный доступ к вашему устройству или сети.

Сильные пароли и регулярное их обновление:

Создание сложных паролей и их регулярное обновление уменьшает риск несанкционированного доступа к вашим учетным записям.

Многофакторная аутентификация:

Использование нескольких методов подтверждения личности, таких как пароль и код из SMS, повышает уровень безопасности.

Обновление Программного Обеспечения:

Регулярное обновление операционных систем, браузеров, антивирусных программ и другого программного обеспечения помогает закрывать уязвимости и обеспечивать безопасность.

Разграничение прав пользователей:

Назначение минимально необходимых прав пользователям ограничивает возможности злоумышленников при несанкционированном доступе.

Безопасное подключение к интернету:

Использование безопасных сетей, виртуальных частных сетей (ВПН) и протоколов шифрования помогает предотвращать перехват данных при передаче через общественные сети.

Резервное копирование данных:

Регулярное создание резервных копий важных данных помогает восстановлению информации в случае воздействия вредоносных программ или других технических сбоев.

Мониторинг и анализ событий:

Системы мониторинга и анализа событий позволяют выявлять аномалии и потенциальные угрозы в реальном времени.

Эффективное сочетание этих мер позволяет улучшить уровень защиты от технических рисков и поддерживать безопасность цифровой среды.

2.3. ПОТРЕБИТЕЛЬСКИЕ РИСКИ

Потребительские риски представляют собой возможность потери или негативного воздействия на интересы потребителя при приобретении товаров или услуг. В контексте злоупотребления правами потребителя в интернете, эти риски могут быть усугублены различными аспектами. Давайте рассмотрим несколько типичных потребительских рисков, связанных с интернет-покупками, и приведем примеры:

• Приобретение товара низкого качества: Покупка электроники или одежды онлайн, которая оказывается не соответствующей заявленным характеристикам или фотографиям. Например, покупка смартфона с нефункциональной камерой.

• Приобретение поддельного товара: Приобретение фальшивых брендов или подделок товаров. Например, заказ дизайнерской сумки, которая оказывается подделкой.

• Потеря денежных средств: Предоплата за товар или услугу, но не получение их в дальнейшем. Например, оплата за билеты на концерт через мошеннический веб-сайт, который не предоставляет билеты.

• Хищение персональной информации: Ввод личных данных на поддельных сайтах, что может привести к утечке личной информации и использованию ее злоумышленниками. Например, предоставление кредитной карты на мошенническом сайте.

Рассмотрим некоторые общие признаки, на которые стоит обратить внимание при совершении покупок или использовании услуг:

• Сомнительная репутация продавца или поставщика: Негативные отзывы и оценки от других потребителей. Отсутствие информации о компании или продавце.

• Неясные условия сделки: Неполные или неясные условия продажи или предоставления услуг. Скрытые платежи или дополнительные комиссии. Оплата переводом на карту.

• Низкая степень безопасности в онлайн-среде: Отсутствие защищенного соединения (HTTPS) при совершении онлайн-платежей. Недостаток информации о мерах безопасности, принимаемых продавцом или сервисом.

• Предложения, звучащие слишком хорошо: Слишком низкие цены на популярные товары или услуги. Обещания высоких доходов или быстрого обогащения.

• Отсутствие контактной информации: Отсутствие или недостоверность контактной информации (телефон, адрес, электронная почта).

• Исключительная предоплата: Требование полной предоплаты без гарантии получения товара или услуги.

• Запрос на предоставление избыточной личной информации без явной необходимости.

• Просьбы перейти для обсуждения процесса покупки в личные сообщения в мессенджерах.

• Недостоверная или подозрительная продукция: Отсутствие подлинных отзывов или подтверждений о качестве продукции. Неясная или сомнительная история происхождения товара.

• Отсутствие политики возврата или гарантии: Отсутствие информации о том, как решаются проблемы с продукцией или услугами. Отказ продавца или поставщика от ответственности.

При обнаружении подобных признаков важно быть бдительным и, при необходимости, обратиться за дополнительной проверкой или поддержкой.

Как обезопасить себя:

• Используйте надежные платформы: Покупайте товары и услуги только на проверенных и известных онлайн-площадках.

• Проверяйте отзывы: Перед покупкой ознакомьтесь с отзывами других покупателей о продавцах, продукции или услугах.

• Будьте бдительны при предоставлении личной информации:

Никогда не раскрывайте свои личные данные на ненадежных сайтах или через ненадежные каналы.

• Используйте безопасные методы оплаты: Предпочтительно использовать кредитные карты или другие защищенные методы оплаты, которые предоставляют возможность оспаривания транзакций.

Что делать, если стали жертвой:

• Свяжитесь с банком: Если произошла финансовая афера, сообщите своему банку или провайдеру платежей, чтобы заблокировать дальнейшие транзакции.

• Измените пароли: Измените пароли к своим учетным записям на сайтах, где могла быть компрометирована ваша информация.

• Сообщите в полицию: Подайте жалобу в местное правоохранительное учреждение и предоставьте им всю доступную информацию о случившемся.

• Сообщите в онлайн-платформу: Если проблема связана с онлайн-покупками, обратитесь в службу поддержки платформы и дайте им знать о ситуации.

• Получите консультацию: Обратитесь за консультацией к юристу или организации, занимающейся защитой прав потребителей, чтобы узнать о возможных шагах для восстановления ущерба.

2.3. КОНТЕНТНЫЕ РИСКИ

Контентные риски представляют собой потенциальные опасности и негативные последствия, связанные с использованием контента, доступного в интернете. Эти риски могут возникнуть при взаимодействии пользователей с разнообразными материалами, такими как тексты, изображения, аудио- и видеофайлы, а также ссылки на различные ресурсы. Ниже представлены примеры контентных рисков:

1. Недостоверная информация, фейки

2. Материалы сексуального характера

3. Информация, содержащая жестокость, насилие или агрессию, шокирующий контент

4. Пропаганда наркотиков, алкоголя, сигарет, самоубийств, опасных способов похудания

Общие признаки контентных рисков могут включать в себя следующие характеристики:

• Скрытность и маскировка: Материалы могут быть представлены в скрытой или маскированной форме, затрудняя их распознавание на первый взгляд.

• Эмоциональная нагрузка: Контент может вызывать сильные эмоциональные реакции, такие как шок, страх, отвращение или восторг, что может быть использовано для удержания внимания.

• Недостаток источников и подтверждения: Материалы часто могут появляться без четких источников или подтверждений, что

затрудняет проверку их достоверности.

• Привлекательность и популярность: Контент, нацеленный на массовую аудиторию и обладающий высокой степенью визуальной или эмоциональной привлекательности, может активнее распространяться.

• Разнообразие форматов: Рискованный контент может принимать различные формы, включая тексты, изображения, видео, аудио и другие медийные форматы.

• Отсутствие цензуры и нарушение норм: Контент может содержать нецензурные выражения, нарушать нормы общепринятого поведения и представлять собой нарушение этических стандартов.

• Специфическая целевая аудитория: Пропагандистские материалы могут быть направлены на определенные группы, такие как подростки, чтобы оказать более сильное влияние на их восприятие и поведение.

Для обеспечения безопасности и минимизации воздействия этих рисков важно развивать медиаграмотность, умение критически оценивать контент, быть осведомленным о нормах и этических стандартах, а также устанавливать контроль над своими онлайн-привычками.

Рассмотрим каждый риск подробнее.

Недостоверная информация (фейки)

Недостоверная информация, или фейковые новости (от англ. «fake» - подделка), представляют собой ложные или искаженные сведения, распространяемые с целью ввести в заблуждение общественность. Эти материалы могут быть созданы с различными целями, такими как манипуляция общественным мнением, дезинформация, политическая пропаганда или просто для привлечения внимания.

Опасности:

• Введение в заблуждение: Фейки могут искажать факты и события, вводя людей в заблуждение и создавая искаженное представление о реальности.

• Подрыв доверия: Распространение фейковых новостей может подрывать доверие к информационным источникам, включая традиционные СМИ и онлайн-ресурсы.

• Разжигание напряженности: Фейковые материалы могут быть использованы для создания напряженности в обществе, раскола между группами людей или даже провокации конфликтов.

Особенности:

• Сложность проверки: Фейки могут быть трудными для проверки, особенно если они созданы с использованием поддельных фотографий, видео или документов.

• Быстрое распространение: Социальные сети и другие онлайн-платформы способствуют быстрому распространению фейков, что затрудняет контроль и предотвращение их дальнейшего распространения.

Как себя обезопасить:

• Проверяйте источники: Перед тем как поделиться информацией, удостоверьтесь в ее достоверности, проверяя несколько источников.

• Обратите внимание на подозрительные заголовки: Фейковые новости часто имеют сенсационные заголовки, написанные так, чтобы привлечь внимание.

• Проверяйте факты: Воспользуйтесь фактчекинговыми ресурсами, которые анализируют и проверяют достоверность информации.

• Будьте критичными потребителями информации: Развивайте критическое мышление и сомневайтесь в информации, если что-то кажется слишком удивительным или подозрительным.

• Обучение медиаграмотности: Обучение основам медиаграмотности помогает людям различать надежные источники информации от ненадежных.

Соблюдение этих мер позволяет уменьшить риск попадания

в заблуждение и способствует формированию осознанного подхода к потреблению информации в цифровом мире.

Материалы сексуального характера

Материалы сексуального характера включают в себя контент, предназначенный для вызова сексуального интереса или удовлетворения. Это может быть порнография, эротические изображения, аудио- и видеоматериалы, а также другие формы сексуального контента.

Опасности:

• Воздействие на психологическое здоровье: Избыточное потребление сексуального контента может влиять на психологическое здоровье, вызывая зависимость, дисфункции или негативное воздействие на отношения.

• Небезопасное поведение: Неконтролируемое потребление материалов сексуального характера может способствовать развитию небезопасных сексуальных практик, а также повышать риск заболеваний.

• Воздействие на молодежь: Доступ детей и подростков к материалам сексуального характера может вызывать преждевременное сексуальное развитие и негативно влиять на формирование их взглядов на секс и отношения.

Негативные проявления:

• Нежелательные ситуации: Неконтролируемое распространение интимного контента может привести к нежелательным ситуациям, таким как месть порнографией, когда интимные материалы становятся доступными широкой аудитории без согласия заснятых лиц.

• Зависимость: Возможно развитие зависимости от сексуального контента, что может негативно сказаться на психическом здоровье.

Как себя обезопасить:

• Установка контроля доступа: Используйте средства контроля доступа, такие как пароли или настройки безопасности, чтобы ограничить доступ к контенту для определенных групп пользователей.

• Контроль времени онлайн: Ограничивайте время, проведенное в онлайне, особенно в отношении доступа к материалам сексуального характера.

• Фильтры и блокировки: Используйте фильтры контента и программы блокировки, чтобы ограничить доступ к материалам сексуального характера.

• Осведомленность и образование: Понимание воздействия сексуального контента на психологическое здоровье может помочь соблюдать здоровые границы и разумно использовать такой контент.

• Обсуждение с детьми и подростками: Родители должны обсудить с детьми вопросы, связанные с сексуальностью, объяснить возможные риски и поощрять здоровое отношение к телесности и сексу.

Будьте внимательны к своему психическому здоровью, устанавливайте границы и принимайте меры для обеспечения безопасного использования интернета.

Информация, содержащая жестокость, насилие или агрессию, шокирующий контент:

Включает в себя материалы, которые демонстрируют или описывают акты жестокости, насилия, агрессии или другие шокирующие сцены. Это может быть в виде видео, фотографий, текстов или звуков, предназначенных для вызова сильных эмоциональных реакций.

Опасности:

• Психологическое воздействие: Просмотр жестокого или на-

сильственного контента может оказать сильное психологическое воздействие, вызвав стресс, тревогу и даже травматические последствия.

• Уменьшение чувствительности к насилию: Постоянное воздействие на насильственный контент может привести к десенсибилизации — уменьшению чувствительности к насилию, что может снизить эмпатию и сочувствие.

• Поощрение агрессии: Некоторый контент может поощрять агрессивное поведение, особенно у уязвимых групп, таких как подростки.

Проявления:

• Жестокие сцены и изображения: Насильственные или шокирующие сцены, такие как физическое насилие, жестокость над животными или травмирующие события.

• Угрозы и агрессивные высказывания: Текстовые или звуковые материалы, содержащие угрозы, агрессивные заявления или призывы к насилию.

Как себя обезопасить:

• Контроль контента: Используйте фильтры и блокировки, чтобы ограничивать доступ к материалам, содержащим жестокость или насилие.

• Ограничение времени просмотра: Ограничьте время, проводимое в интернете, чтобы уменьшить возможность случайного столкновения с шокирующим контентом.

• Предупреждения и этические стандарты: Обратите внимание на предупреждения о содержании, прежде чем просматривать материалы, и поддерживайте этические стандарты в сети.

• Развитие медиаграмотности: Обучение умениям анализа и оценки контента помогает различать шокирующий контент от безопасного.

• Консультации и поддержка: Если контент вызывает стресс или тревогу, обратитесь за помощью к специалистам или обратитесь к доверенным людям для поддержки.

Важно подчеркнуть, что забота о себе и осознанное взаимодействие с контентом помогут предотвратить негативные эмоциональные последствия и поддерживать психическое здоровье.

Пропаганда наркотиков, алкоголя, сигарет, самоубийств, опасных способов похудания:

Заключается в представлении и распространении информации, поощряющей употребление наркотиков, алкоголя, курение, самоповреждение или опасные методы похудания. Пропаганда такого рода может включать в себя контент, стимулирующий или романтизирующий эти вредные практики.

Опасности:

• Здоровье и благополучие: Пропаганда вредных привычек может привести к серьезным проблемам здоровья и безопасности, таким как зависимость, болезни и даже смерть.

• Манипуляция: Ложная или искаженная информация о вредных практиках может манипулировать людьми, заставляя их принимать небезопасные решения.

• Влияние на молодежь: Молодые люди, особенно подростки, могут быть более уязвимыми к воздействию пропаганды, что может повлиять на формирование их взглядов и поведения.

Проявления:

• Реклама вредных товаров: Продвижение наркотиков, алкоголя, табака и других вредных товаров через рекламу и маркетинг.

• Публичные высказывания и изображения: Видео, тексты или изображения, романтизирующие опасные практики или пропагандирующие их использование.

Как себя обезопасить:

• Критическое мышление: Развивайте критическое мышление и умение анализа информации, чтобы распознавать манипуляции и искажения в пропагандистских материалах.

• Образование и информирование: Познакомьтесь с фактами о вреде наркотиков, алкоголя, курения и других вредных привычек, чтобы лучше понимать их негативные последствия.

• Ограничение доступа: Используйте средства контроля доступа и фильтры контента, чтобы ограничить ваше воздействие от пропагандистских материалов.

• Развитие силы воли: Укрепление силы воли и умение управлять стрессом и трудностями помогут сопротивляться влиянию пропаганды.

• Поддержка окружения: Развивайте сеть поддержки в виде друзей, семьи и сообщества, где можно обсудить вопросы здоровья и безопасности.

Обучение медиаграмотности и образование в сфере здоровья помогают людям различать положительные и негативные воздействия информации и принимать более информированные решения о своем поведении и здоровье.

Что делать, если вы столкнулись с контентными рисками?

Если вы столкнулись с указанными контентными рисками в интернете, важно принять некоторые шаги для минимизации негативных последствий и обеспечения своей безопасности. Вот несколько рекомендаций:

1. Сохраните спокойствие. Не торопитесь реагировать эмоционально. Попытайтесь сохранить спокойствие и рациональность.

2. Прекратите взаимодействие с контентом, вызвавшим беспокойство или риск. Закройте вкладку, прекратите просмотр или

прекратите взаимодействие с соответствующим ресурсом.

3. Удалите контент. Если это возможно, удалите или скройте контент, который вызывает беспокойство или представляет риск.

4. Обновите свои учетные данные. Если риск связан с конфиденциальной информацией, обновите свои пароли и примите меры безопасности для защиты своей учетной записи.

5. Запишите детали. Если возможно, запишите детали ситуации: где и когда это произошло, что именно вы видели или прочитали, и как это повлияло на вас.

6. Сообщите об инциденте. Если контент является незаконным или нарушает политику платформы, на которой вы его обнаружили, сообщите об этом администрации сайта или службе поддержки.

7. Используйте средства безопасности. Если возможно, воспользуйтесь средствами блокировки, фильтров и настроек конфиденциальности, чтобы предотвратить дальнейшее воздействие подобного контента.

8. Поделитесь с кем-то. Расскажите о ситуации доверенному человеку, например, близкому другу, члену семьи или коллеге. Обсудите свои ощущения и опасения.

9. Проконсультируйтесь с профессионалами. Если сталкиваетесь с трудностями в управлении своими эмоциями или переживаете психологический стресс, обратитесь за помощью к психотерапевту, консультанту по психологической помощи или к другим специалистам.

Запомните, что ваше благополучие важнее всего. Если вы не уверены, что делать, и чувствуете, что ситуация выходит из-под контроля, не стесняйтесь обратиться за профессиональной помощью.

2.4. КОММУНИКАЦИОННЫЕ РИСКИ

Коммуникационные риски - это потенциальные негативные последствия или угрозы, связанные с обменом информацией и взаимодействием в онлайн-пространстве. Эти риски могут проявляться различными способами и воздействовать на уровне безопасности, приватности, репутации и эмоционального состояния участников виртуального общения.

Общие признаки коммуникационных рисков могут варьироваться в зависимости от контекста, но вот несколько общих признаков, которые могут указывать на возникновение опасных ситуаций:

1. Негативный тон и содержание. Наличие угроз, оскорблений, оскорбительных комментариев или ненавистных высказываний. Проявление агрессии, недружелюбия или неуважения в общении.

2. Навязчивость и нарушение границ: Нежелательные попытки вмешательства в личную жизнь. Навязчивые запросы на личные данные, финансовую помощь или другие привилегии.

3. Использование давления и шантажа: Угрозы физического или эмоционального воздействия. Попытки вынудить к действиям, которые человек не хочет совершать.

4. Ложная идентификация и мошенничество: Поддельные профили или маскировка под другого человека. Запросы на финансовую помощь или предоставление ложной информации.

5. Непонятное поведение: Недостаток ясности в коммуникации, что может создать путаницу или недопонимание. Использование двусмысленных высказываний или уклонение от конкретных вопросов.

6. Изменение в поведении собеседника: Резкое изменение в стиле общения, появление угроз, агрессии или навязчивости может быть признаком опасной ситуации.

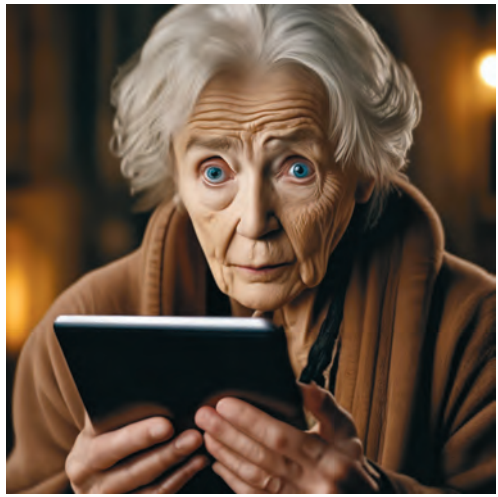
7. Интенсивное наблюдение и сталкинг: Навязчивые попытки отслеживания действий и местоположения. Повторные попытки установить контакт, несмотря на явное желание избежать общения.

8. Отклонение от цифровой этики: Нарушение правил цифрового общения, таких как распространение ложной информации, агрессивное общение.

9. Чувство дискомфорта или беспокойства: Если вы чувствуете дискомфорт, беспокойство или страх в процессе общения, это может быть признаком рискованной ситуации.

10. Негативные эмоции: Если ваши эмоции в ответ на коммуникацию включают страх, раздражение, тревогу или депрессию, это может указывать на рискованный характер общения.

11. Непонятные мотивы и цели: Если намерения собеседника кажутся непонятными или подозрительными, возможно, вы сталкиваетесь с рискованной ситуацией.



12. Интуиция: Доверьтесь своей интуиции. Если что-то кажется «не так» или вызывает сомнения, возможно, стоит быть настороже.

Важно осознавать свои границы, доверять своей интуиции и в случае необходимости принимать меры для обеспечения своей безопасности и комфорта в онлайн-и офлайн-средах общения.

Приведем несколько примеров коммуникационных рисков в цифровой среде:

• Кибербуллинг. Оскорбления, угрозы и насмешки в онлайн-среде, направленные на конкретного пользователя. Например, размещение оскорбительных комментариев на странице социальной сети, целью унижения и вызова эмоционального стресса.

• Преследование в цифровой среде. Навязчивое следование за пользователем в Интернете, мониторинг его действий, а также нежелательные попытки связи. Например, онлайн-сталкерство, многократные попытки вторжения в личное пространство пользователя.

• Цифровая дискриминация. Дискриминация или негативное отношение к пользователям на основе их цифровой активности. Например, оскорбления или угрозы, направленные на определенную группу людей из-за их характеристик, выраженных в онлайне.

• Нарушение приватности. Несанкционированный доступ к личной информации или разглашение частной переписки. Например, взлом аккаунта с целью получения личных данных или распространение чужих личных сообщений без согласия.

• Репутационные риски. Негативные последствия, связанные с ущемлением репутации пользователя в онлайн-среде, часто вызванные распространением недостоверной или компрометирующей информации.

• Кража личности. Использование чужой личной информации для мошенничества или создания поддельных аккаунтов. Например воровство и использование персональных данных для открытия банковских счетов или получения кредитов.

• Онлайн-знакомства. Риски, связанные с встречей с незнакомцами, впервые познакомившимися в сети. Например, встреча с онлайн-знакомым без предварительной проверки его личности и намерений может привести к опасным последствиям.

Рассмотрим данные риски подробнее.

Кибербуллинг

Это форма агрессии и жестокости, совершаемая через цифровые средства коммуникации, такие как социальные сети, сообщения, электронная почта и т.д. Кибербуллинг включает в себя намеренное и систематическое медленное мучение, угрозы, оскорбления, распространение ложной информации и другие формы цифровой жестокости.

Проявления кибербуллинга могут включать в себя:

• Оскорбительные комментарии: Нападки на внешность, интеллект, вероисповедание и т.д.

• Угрозы: Высказывания о возможном вреде, как физическом, так и эмоциональном.

• Распространение слухов и ложной информации: Создание и распространение фейковых новостей, фотографий или видео с целью унижения.

• Имитация личности: Создание поддельных профилей для оскорбительных или провокационных целей.

• Изоляция и исключение: Исключение из общественных групп, создание ощущения изоляции.

Последствия кибербуллинга включают в себя:

• Психологические проблемы: Стресс, депрессия, тревожные расстройства и даже мысли о самоубийстве у пострадавших.

• Социальные проблемы: Изоляция, ухудшение отношений с окружающими.

• Физическая опасность: В некоторых случаях кибербуллинг может перейти в реальные угрозы и физическое насилие.

Как обезопасить себя от кибербуллинга:

1. Будьте бдительными с личной информацией: Не раскрывайте слишком много о себе в сети.

2. Устанавливайте ограничения на конфиденциальность: Настройте параметры конфиденциальности в социальных сетях.

3. Не вступайте в конфликты: Избегайте участия в онлайн-спорах, не реагируйте на провокации.

4. Блокировка и информирование: Заблокируйте пользователей, совершающих кибербуллинг, и сообщите об этом администраторам платформы.

5. Сохраняйте доказательства: Если вы стали жертвой, сохраните скриншоты оскорбительных сообщений как доказательство.

Что делать, если стали жертвой кибербуллинга:

1. Не молчите: Обратитесь за помощью к доверенным взрослым, родителям, учителям.

2. Заведите доказательства: Сохраните доказательства кибербуллинга, включая скриншоты и ссылки.

3. Блокируйте и репортите: Заблокируйте агрессора и сообщите

о случае администраторам социальной сети.

4. Обратитесь за помощью: Поговорите с профессионалами, такими как психологи или консультанты, чтобы справиться с эмоциональными последствиями.

Что делать, если вы стали свидетелем кибербуллинга

Если вы стали свидетелем кибербуллинга, важно предпринять действия, чтобы помочь остановить агрессивное поведение и поддержать жертву. Вот несколько шагов, которые вы можете предпринять:

1. Не молчите: Не игнорируйте случаи кибербуллинга. Если вы видите оскорбительные комментарии или угрозы, не оставайтесь равнодушными.

2. Соберите доказательства: Сделайте скриншоты оскорбительных сообщений или любых других проявлений кибербуллинга. Это может быть полезным в случае необходимости предоставления доказательств.

3. Поддержите жертву: Выразите свою поддержку жертве, покажите, что она не одна. Эмоциональная поддержка может быть важным аспектом в борьбе с негативными последствиями кибербуллинга.

4. Пожалуйтесь на сообщения: Если платформа, на которой происходит кибербуллинг, предоставляет инструменты для блокировки или сообщения о нарушениях, используйте их. Это поможет ограничить доступ агрессора к жертве.

5. Сообщите администраторам: Сообщите о случае администраторам социальной сети или платформы. Многие онлайн-сервисы имеют политику борьбы с кибербуллингом и могут принять меры в отношении агрессора.

Важно помнить, что активное вмешательство и поддержка могут помочь предотвратить дальнейшее распространение кибербуллинга и содействовать созданию безопасной и поддерживающей онлайн-среды.

Преследование в цифровой среде (онлайн-преследование)

Представляет собой навязчивое следование за пользователем

в Интернете, мониторинг его действий, а также нежелательные попытки связи. Это поведение может быть угрожающим и вызывать чувство страха у жертвы.

Проявления преследования в цифровой среде могут включать в себя:

1. Нежелательные сообщения: Постоянные сообщения через электронную почту, социальные сети или мессенджеры.

2. Мониторинг онлайн-активности: Слежение за активностью в социальных сетях, блогах или форумах без согласия пользователя.

3. Создание поддельных профилей: Преследователь может создавать поддельные аккаунты для наблюдения за жертвой анонимно.

4. Слежение в реальной жизни: Комментарии или угрозы, указывающие на то, что преследователь следит за жертвой в реальной жизни.

5. Угрозы и шантаж: Использование угроз или попыток шантажа для контроля над жертвой.

Опасности преследования в цифровой среде включают в себя:

• Угроза личной безопасности: Преследование может стать реальной угрозой для физической безопасности жертвы.

• Психологическое давление: Навязчивые действия могут привести к чувству беспокойства, стресса и тревоги.

• Потеря приватности: Преследование нарушает личную жизнь и чувство безопасности в онлайн-пространстве.

Как обезопасить себя от преследования в цифровой среде:

• Настройте приватность: Убедитесь, что настройки приватности в социальных сетях и других онлайн-платформах установлены на максимальный уровень.

• Блокируйте нежелательные контакты: Заблокируйте преследователя, чтобы ограничить его доступ к вашим данным и активности.

• Не делитесь личной информацией: Избегайте публикации чувствительной информации, такой как местоположение, контакт-

ные данные и детали вашей повседневной жизни.

• Будьте осторожны с новыми контактами: Не добавляйте в друзья или не общайтесь с незнакомцами без должной осторожности.

Что делать, если стали жертвой преследования в цифровой среде:

1. Сообщите об этом: Сообщите о случае преследования администраторам социальных сетей или платформы.

2. Сохраняйте доказательства: Сделайте скриншоты или сохраните сообщения в качестве доказательств.

3. Блокируйте и ограничивайте доступ: Заблокируйте преследователя, ограничьте видимость своих данных и контента.

4. Обратитесь за помощью: Сообщите о случае преследования взрослым, таким как родителям, учителям или другим доверенным лицам.

5. Обратитесь в правоохранительные органы: Если преследование становится серьезным, обратитесь за помощью в местные правоохранительные органы.

Важно подчеркнуть, что преследование в цифровой среде является серьезным преступлением, и вмешательство правоохранительных органов может быть необходимым для обеспечения безопасности жертвы.

Цифровая дискриминация

Это форма дискриминации, основанная на цифровых технологиях и присущая онлайн-пространству. Это может включать в себя негативное отношение, навязчивые действия или иные формы преследования, основанные на расовой, гендерной, социальной, религиозной или иной характеристике человека.

Проявления цифровой дискриминации могут включать в себя:

• Оскорбительные комментарии: Негативные высказывания, направленные на личные характеристики, такие как раса, пол, вероисповедание и т.д.

• Ограничение доступа: Отказ в предоставлении равных возможностей, доступа или участия в определенных онлайн-сообществах или сервисах.

• Цифровой буллинг: Онлайн-буллинг или домогательства, основанные на различиях в личных характеристиках.

• Распространение стереотипов: Создание и распространение стереотипов через цифровые средства для ущемления определенных групп людей.

• Интернет-троллинг: Провокационное поведение с целью вызвать отрицательные реакции или поддержать дискриминацию.

Последствия цифровой дискриминации включают в себя:

• Угроза безопасности: Неконтролируемые высказывания или действия могут представлять угрозу для физической или психической безопасности.

• Эмоциональные последствия: Жертва может испытывать стресс, депрессию и чувство изоляции из-за дискриминации.

• Ущемление прав и возможностей: Ограничение доступа к ресурсам, информации или возможностей из-за дискриминации.

Как обезопасить себя от цифровой дискриминации:

• Будьте осторожны с личной информацией: Ограничьте раскрытие личных данных в сети, чтобы уменьшить возможность дискриминации.

• Настройте приватность: Используйте настройки приватности в социальных сетях и других онлайн-платформах для контроля за тем, кто видит вашу информацию.

• Блокируйте агрессоров и сообщайте администрации: Заблокируйте тех, кто проявляет к вам агрессию и сообщите о случаях дискриминации на соответствующих платформах. Это может помочь в пресечении негативного поведения.

Что делать, если стали жертвой цифровой дискриминации:

1. Сохраните доказательства: Сделайте скриншоты или сохраните сообщения, демонстрирующие дискриминацию.

2. Сообщите об инциденте: Обратитесь к администраторам платформы, чтобы сообщить о дискриминации и запросить поддержку.

3. Поделитесь с доверенными лицами: Расскажите о случае дискриминации доверенным друзьям, семье или коллегам.

4. Обратитесь к профессионалам: Если дискриминация становится серьезной проблемой, обратитесь к юристам или организациям, специализирующимся на правах человека и цифровой безопасности.

Нарушение приватности

Это незаконное или несанкционированное вмешательство в личную жизнь человека, когда его личные данные, информация или действия раскрываются без его согласия. Это может происходить как в реальной жизни, так и в цифровой среде.

Проявления нарушения приватности могут включать в себя:

• Незаконный доступ к личной информации: Взлом электронных учетных записей, почты или социальных сетей.

• Разглашение конфиденциальных данных: Раскрытие личной информации, такой как адрес, номер телефона, финансовые данные без согласия.

• Шпионаж и слежка: Скрытое наблюдение, слежка за человеком в реальной жизни или онлайн.

• Кража личности: Использование чужой личной информации для мошенничества, открытия счетов, получения кредитов и других противоправных действий.

• Мониторинг онлайн-активности: Слежение за действиями пользователя в интернете без его согласия.

Опасности нарушения приватности включают в себя:

• Финансовые потери: Кража финансовых данных может привести к финансовым убыткам и мошенничеству.

• Эмоциональные последствия: Люди могут испытывать стресс и тревогу из-за потери контроля над своей личной информацией.

• Угроза безопасности: Нарушение приватности может приве-

сти к реальным угрозам физической безопасности.

• Потеря репутации: Разглашение личной информации может повлиять на репутацию человека в профессиональной и личной сферах.

• Идентификационный воровство: Кража личности может привести к серьезным последствиям, таким как открытие счетов, получение кредитов и другие финансовые махинации.

Как обезопасить себя от нарушения приватности:

• Сильные пароли и двухфакторная аутентификация: Используйте сложные пароли и включите двухфакторную аутентификацию для дополнительного уровня безопасности.

• Настройте приватность: Установите строгие параметры конфиденциальности в социальных сетях и онлайн-профилях.

• Будьте бдительны в сети: Избегайте раскрытия чувствительной информации, будьте внимательны к ссылкам и запросам на личные данные.

• Регулярно проверяйте финансовые отчеты: Мониторьте свои финансовые отчеты на предмет подозрительной активности.

• Обновляйте программное обеспечение: Регулярно обновляйте программы и операционные системы, чтобы устранить уязвимости.

Что делать, если стали жертвой нарушения приватности:

1. Смените пароли: Измените пароли ко всем учетным записям, которые могли быть скомпрометированы.

2. Сообщите официальным органам: Обратитесь в правоохранительные органы и уведомите о нарушении приватности.

3. Свяжитесь с банком: Если касается финансов, свяжитесь с банком и сообщите о возможной краже личных данных.

4. Обратитесь к специалистам по кибербезопасности: Получите консультацию у профессионалов по кибербезопасности, чтобы

устранить угрозы и предотвратить будущие инциденты.

Репутационные риски

Это угрозы, которые могут повлиять на хорошую репутацию личности, компании или организации. Они проявляются через различные ситуации и действия, которые могут создать негативное восприятие со стороны окружающих.

Проявления репутационных рисков:

• Распространение ложной информации: Нападки, клевета и распространение заведомо ложных сведений о человеке или компании.

• Манипуляции в социальных сетях: Атаки на репутацию через поддельные аккаунты, троллинг, массовые отрицательные комментарии или широкое распространение негативных материалов.

• Цифровые домогательства: Систематическое и агрессивное поведение в онлайне с целью вызвать эмоциональные или психологические травмы.

• Угрозы и шантаж: Попытки заставить человека совершить определенные действия под угрозой раскрытия компрометирующей информации.

• Негативные рецензии и отзывы: Массированное публикование отрицательных отзывов, даже если они не соответствуют действительности, с целью подорвать репутацию.

Опасности репутационных рисков:

• Потеря доверия: Негативная репутация может привести к потере доверия со стороны клиентов, партнеров, коллег и общественности.

• Финансовые потери: Уменьшение клиентской базы, отказ инвесторов или клиентов из-за негативной репутации может привести к финансовым потерям.

• Ухудшение бренда: Негативная репутация может оказать влияние на общее восприятие бренда, затрудняя привлечение новых клиентов и партнеров.

• Проблемы в карьере: Для частных лиц репутационные риски

могут сказаться на карьерных возможностях, поиск работы или отношениях в профессиональном сообществе.

Как обезопасить себя от репутационных рисков:

• Цифровая грамотность: Развивайте навыки цифровой грамотности, чтобы эффективно управлять своим онлайн-присутствием.

• Бдительность в сети: Будьте осторожными с тем, что вы размещаете в сети, и с кем взаимодействуете.

• Мониторинг репутации: Регулярно проверяйте отзывы, упоминания и обсуждения в сети, чтобы оперативно реагировать на негатив.

• Сильные пароли и безопасность аккаунтов: Защищайте свои онлайн-аккаунты сильными паролями и используйте дополнительные методы аутентификации.

• Обратитесь за юридической помощью: В случае клеветы или распространения ложной информации рассмотрите возможность обращения за юридической поддержкой.

Что делать, если стали жертвой:

1. Не паникуйте: Сначала сохраните спокойствие и изучите обстановку.

2. Анализируйте источник: Определите, откуда идет угроза и какие именно данные подвергаются риску.

3. Свяжитесь с профессионалами: Обратитесь за помощью к специалистам по цифровой безопасности, юристам или репутационным менеджерам.

4. Реагируйте адекватно: Не отвечайте на агрессию агрессией. Профессиональный и адекватный ответ может помочь в восстановлении репутации.

5. Используйте позитивный контент: Размещайте позитивный контент о себе или компании, чтобы смягчить негативные впечатления.

6. Следите за развитием событий: Мониторьте реакции окружающих и анализируйте эффективность предпринятых мер.

7. При необходимости, воспользуйтесь правовыми или техниче-

скими средствами для защиты своей репутации.

Кража личности

Это преступление, при котором злоумышленник использует личные данные человека без его согласия с целью получения финансовой выгоды, проведения мошенничества или совершения других противоправных действий от его имени.

Проявления кражи личности могут включать в себя:

• Финансовые махинации: Открытие банковских счетов, получение кредитов или кредитных карт от имени пострадавшего.

• Медицинский мошенничество: Использование личных данных для получения медицинских услуг или страховки.

• Использование личных данных в сети: Регистрация на веб-сайтах, социальных сетях или форумах от имени жертвы.

• Налоговые махинации: Подача налоговых деклараций от имени пострадавшего с целью получения возврата налогов.

• Преступления в сфере труда: Получение работы или предоставление ложной информации о занятости с использованием личных данных.

Опасности кражи личности включают в себя:

• Финансовые убытки: Пострадавший может потерять деньги из-за мошеннических транзакций.

• Репутационные проблемы: В результате кражи личности могут появиться проблемы с репутацией, особенно если злоумышленник совершает преступления от имени жертвы.

• Психологические и эмоциональные последствия: Жертва может испытывать стресс, беспокойство и тревогу из-за нарушения своей приватности.

• Потеря контроля над личными данными: Кража личности влечет за собой утрату контроля над своей личной информацией, что может привести к долгосрочным последствиям.

Как обезопасить себя от кражи личности:

• Сильные пароли: Используйте уникальные и сложные пароли для различных онлайн-сервисов.

• Двухфакторная аутентификация: Включите двухфакторную аутентификацию для дополнительного уровня защиты.

• Мониторинг финансов: Регулярно проверяйте свои банковские и финансовые отчеты на предмет несанкционированных операций.

• Осторожность в сети: Будьте внимательны при предоставлении личной информации онлайн, особенно на ненадежных веб-сайтах.

• Антивирусная защита: Устанавливайте и регулярно обновляйте программы антивирусной защиты для предотвращения вредоносных программ.

Что делать, если стали жертвой кражи личности:

1. Смените пароли: Измените пароли ко всем своим онлайн-учетным записям.

2. Сообщите своим контактам: Сообщите своим контактам, связанным с учетной записью, что вы подверглись взлому и сообщения от вашего имени могли рассылать злоумышленики.

3. Свяжитесь с банком: Уведомите свой банк о случившемся и запросите блокировку счетов или карт.

4. Обратитесь в правоохранительные органы: Сообщите о случае кражи личности в местные правоохранительные органы.

5. Получите юридическую помощь: При необходимости проконсультируйтесь с юристом или агентством по защите от мошенничества.

Риски онлайн-знакомств

Данный тип рисков относится к потенциальным опасностям и негативным последствиям, которые могут возникнуть при использовании интернет-платформ для знакомств. Эти риски могут варьироваться от мошенничества и кибербуллинга до реальных

угроз физической безопасности.

Онлайн-знакомства могут привести к следующим ситуациям:

• Мошенничество: Ложная идентификация, финансовые мошенничества, включая запрос денег или личных данных.

• Кибербуллинг: Оскорбительные комментарии, угрозы и другие формы цифрового насилия.

• Лжепрофили: Создание поддельных профилей с целью обмана или мошенничества.

• Репутационные риски: Распространение ложной информации о вас в онлайн-среде.

• Навязчивость и сталкинг: Нежелательное и навязчивое поведение, следящее за вами в реальной жизни.

• Физическая угроза: Риски встреч с непроверенными и ненадежными собеседниками, что может привести к физической опасности.

Опасности онлайн-знакомств включают в себя:

• Финансовые потери: Мошеннические схемы могут привести к потере денег.

• Физическая безопасность: Встречи с непроверенными людьми могут быть опасными и привести к реальной угрозе безопасности.

• Эмоциональные и психологические последствия: Кибербуллинг и нежелательные отношения могут вызвать стресс и депрессию.

• Репутационные проблемы: Распространение негативной информации о вас может повлиять на вашу репутацию в обществе.

• Угроза личной безопасности: Навязчивые собеседники или сталкеры могут представлять угрозу для вашей безопасности.

Как обезопасить себя от рисков онлайн-знакомств:

• Будьте осторожны с личной информацией: Избегайте раскры-

тия слишком много информации о себе, такой как адрес, финансовые данные или другие чувствительные сведения.

• Проверяйте подлинность профилей: Старайтесь проверять аутентичность профилей и избегайте встреч с людьми, которых вы не знаете.

• Проводите первые встречи в общественных местах: Если решите встретиться с кем-то лично, делайте это в общественных местах и сообщите друзьям о своих планах.

• Будьте бдительны в отношениях: Опасайтесь подозрительного поведения и запросов о финансовой помощи.

• Используйте проверенные платформы: Предпочитайте использование известных и проверенных приложений и сайтов для знакомств.

• Соблюдайте собственные границы: Не давайте давления собеседникам и не нарушайте свои собственные границы.

Что делать, если стали жертвой рисков онлайн-знакомств:

1. Прекратите взаимодействие: Прекратите общение с человеком, который вызывает беспокойство или создает опасность.

2. Блокируйте и сообщите: Заблокируйте нежелательные контакты и сообщите о проблеме администрации платформы.

3. Сохраняйте доказательства: Если вы сталкиваетесь с кибербуллингом, сохраните доказательства в виде скриншотов и записей.

4. Обратитесь за помощью: Обсудите ситуацию с доверенными друзьями, родственниками или правоохранительными органами, если угроза безопасности серьезная.

5. Обратитесь к специалистам: При необходимости обратитесь за консультацией к профессионалам, таким как юристы или

специалисты по кибербезопасности.

Способы предотвратить коммуникационные риски

Предотвращение коммуникационных рисков важно для обеспечения безопасного и эффективного общения. Вот несколько способов, которые могут помочь в этом:

1. Будьте внимательными с личной информацией: Избегайте раскрытия чувствительных данных, таких как адрес, финансовая информация, номер телефона, если нет уверенности в надежности собеседника.

2. Остерегайтесь предоставления личных данных на ненадежных или непроверенных онлайн-платформах.

3. Установите строгие параметры приватности: Воспользуйтесь настройками приватности в социальных сетях и других онлайн-платформах для контроля за тем, кто видит вашу информацию.

4. Будьте осторожными с подозрительной активностью: Обращайте внимание на подозрительные запросы, личные сообщения или поведение в онлайн-среде. Не кликайте на подозрительные ссылки и не отвечайте на подозрительные запросы.

5. Используйте сильные пароли и двухфакторную аутентификацию: Создавайте уникальные и сложные пароли для различных аккаунтов. Включайте двухфакторную аутентификацию, где это возможно, для дополнительного уровня безопасности.

6. Проверяйте подлинность профилей: Будьте бдительными при общении с незнакомцами в онлайн-пространстве. Проверяйте подлинность профилей, чтобы избежать взаимодействия с потенциальными агрессорами или мошенниками.

7. Проводите первые встречи в общественных местах: Если решите встретиться с кем-то лично, выбирайте общественные и

безопасные места для первой встречи. Сообщите друзьям или близким о своих планах на встречу.

8. Будьте бдительными с кибербуллингом и агрессивным поведением: Немедленно блокируйте агрессоров и сообщайте о случаях кибербуллинга или агрессивного поведения в социальных сетях или на других платформах.

9. Создайте сильный социальный круг: Общайтесь с друзьями и близкими о ваших онлайн-взаимодействиях. Поддерживайте связь с реальными людьми и обменивайтесь опытом по безопасности в сети.

10. Обучение детей и подростков цифровой грамотности: Развивайте у детей и подростков навыки безопасного общения в интернете. Объясняйте им риски и наставляйте на правила безопасного поведения в сети.

11. Обратитесь за поддержкой: В случае возникновения проблем обратитесь за помощью к профессионалам, таким как специалисты по кибербезопасности или правоохранительные органы.

Осознанное и ответственное поведение в онлайн-среде поможет уменьшить риски коммуникации и создать безопасное и положительное общественное пространство.

Что делать, если столкнулся с коммуникационными рисками?

Если вы столкнулись с коммуникационными рисками, важно принимать меры для обеспечения своей безопасности и эффективного управления ситуацией. Вот несколько шагов, которые вы можете предпринять:

1. Прекратите взаимодействие: Если вы общаетесь с кем-то онлайн и ощущаете риски или дискомфорт, прекратите взаимодействие с этим человеком. Блокируйте его, если это возможно.

2. Сохраняйте доказательства: Сделайте скриншоты подозрительных сообщений или активности. Это может быть полезно в случае необходимости предоставления доказательств.

3. Измените настройки приватности: Проверьте и обновите настройки приватности на своих социальных сетях и онлайн-профилях. Убедитесь, что только нужные люди имеют доступ к вашей личной информации.

4. Сообщите администрации платформы: Если неприятные события происходят на конкретной онлайн-платформе, сообщите об этом администрации. Многие платформы имеют механизмы для блокировки или сообщения о нарушениях.

5. Обратитесь за поддержкой: Поделитесь ситуацией с близкими друзьями, родственниками или коллегами. Иметь поддержку со стороны может быть важным.

6. Сообщите в правоохранительные органы: Если вы сталкиваетесь с угрозами физической безопасности или серьезным кибербуллингом, обратитесь в местные правоохранительные органы. Предоставьте им доказательства и описания происходящего.

7. Смените пароли и обеспечьте безопасность аккаунтов: Если существует угроза безопасности ваших онлайн-аккаунтов, смените пароли и включите дополнительные меры безопасности, такие как двухфакторная аутентификация.

8. Получите профессиональную помощь: Если ситуация становится критической, обратитесь за профессиональной консультацией. Специалисты по кибербезопасности, психологи или юристы могут предоставить необходимую помощь.

В случае серьезных угроз, связанных с коммуникационными рисками, важно принимать меры незамедлительно и обращаться за помощью к администрации платформ, соответствующим службам и специалистам.

2.5. Цифровая зависимость

Цифровая зависимость проявляется через несколько характерных признаков, которые часто сопровождаются друг другом. Эти признаки включают:

• Постепенное увеличение времени, проводимого в виртуальном пространстве: Люди постепенно увеличивают количество времени, которое они проводят за компьютером или гаджетами.

• Изменение поведения: Виртуальная реальность начинает заменять активности в реальной жизни, ведя к изменению образа поведения.

• Ухудшение эмоционального состояния без доступа к интернету: Лица, страдающие от виртуальной зависимости, могут испытывать депрессию или другие негативные эмоции при отсутствии доступа к сети, что называется «синдромом отмены».

Эти признаки схожи с зависимостью от наркотиков, где все остальные аспекты жизни становятся второстепенными перед удовлетворением зависимости. Это может привести к деградации личности, проявляющейся в ухудшении умственных способностей, потере навыков общения, агрессивности, а также физических проблемах, таких как головные боли и снижение активности.

Таким образом, виртуальная зависимость может привести к серьезным проблемам, влияя на физическое и психическое здоровье, а также на общественные и межличностные навыки.

В чем опасность цифровой зависимости?

Цифровая зависимость представляет собой серьезную проблему, и ее опасность проявляется в нескольких аспектах:

1. Физическое здоровье: Длительное использование цифровых устройств может привести к различным физическим проблемам, таким как напряжение глаз, головные боли, бессонница, проблемы с позвоночником и риск развития других заболеваний.

2. Психическое здоровье: Цифровая зависимость может влиять на психическое состояние, вызывая стресс, депрессию, тревогу и другие психологические проблемы. Синдром отмены, когда отсутствие доступа к цифровым устройствам вызывает дискомфорт

форт, также является распространенным явлением.

3. Социальная изоляция: Зависимость от цифровых технологий может привести к уменьшению личных контактов и социальной активности. Люди могут предпочитать виртуальное общение реальному, что может привести к изоляции от реального мира.

4. Зависимость и злоупотребление: Постоянное взаимодействие с цифровыми устройствами, социальными сетями, играми и другими онлайн-активностями может привести к зависимости. Злоупотребление цифровыми технологиями может воздействовать на производительность на работе или в учебе, а также на отношения с окружающими.

5. Ухудшение качества жизни: Цифровая зависимость может по-

влиять на общую качества жизни, заменяя реальные, более полноценные виды активности на виртуальные, что может привести к утрате интереса к реальной жизни и ее ценностям.

6. Проблемы безопасности: Постоянное онлайн-присутствие может сопровождаться рисками в области кибербезопасности, такими как кибератаки, кражи личных данных, фишинг и другие угрозы.

7. Снижение производительности: Зависимость от цифровых технологий может отрицательно сказаться на производительности, поскольку постоянные перерывы для использования гаджетов могут мешать выполнению задач.

8. Деградация креативности и критического мышления: Постоянное потребление коротких и поверхностных контентов в интернете может привести к утрате способности к глубокому анализу, критическому мышлению и творческой активности.

9. Воздействие на детей: Дети, подвергающиеся цифровой зависимости, могут столкнуться с проблемами в развитии, ухудшением образовательных результатов и социальной неадаптированностью.

10. Потенциальные последствия для общества: Массовая цифровая зависимость может привести к общественным проблемам, таким как ухудшение межличностных отношений, увеличение уровня агрессии и потеря ценностей общества.

Какие виды цифровой зависимости бывают?

Цифровая зависимость может проявляться в различных формах и на разных платформах. Вот несколько распространенных видов цифровой зависимости:

Игровая зависимость (или гейминг-зависимость) представляет собой патологическое влечение к видеоиграм, которое может оказывать существенное воздействие на жизнь человека. Это со-

стояние часто проявляется через чрезмерное и непрерывное участие в компьютерных играх, что в итоге приводит к негативным последствиям для физического и психического здоровья, образа жизни и социальных взаимоотношений.

Игровая зависимость (или гейминг-зависимость) — это состояние, при котором человек становится патологически зависимым от компьютерных игр, что приводит к серьезным негативным последствиям для его физического и психического здоровья, а также для социальной жизни. Эта зависимость обычно проявляется в чрезмерном и непрерывном участии в видеоиграх.

Признаки игровой зависимости:

• Чрезмерное время, проводимое в играх: Зависимые от игр могут играть в течение многих часов в день, игнорируя другие обязанности и заботы.

• Утрата контроля: Люди могут потерять контроль над количеством времени, проведенным в играх, и не могут остановиться даже в случае наличия других важных дел.

• Отказ от реальных обязанностей: Игроки могут пренебрегать школой, работой, социальными взаимодействиями и другими обязанностями из-за игр.

• Изменения в поведении: Могут появиться изменения в поведении, такие как раздражительность, агрессия или апатия.

• Изоляция от общества: Зависимость от игр может привести к изоляции от реальных социальных контактов, дружб и отношений.

• Физические проблемы: Долгие периоды игр могут вызывать физические проблемы, такие как бессонница, проблемы со спиной, глазами и др.

Причины появления игровой зависимости:

• Психологическая удовлетворенность: Игры могут предостав-

лять психологическую удовлетворенность, эмоциональные высоки и бегство от реальности.

• Социальная изоляция: Игры могут служить способом избегания социальных проблем или трудностей в общении.

• Онлайн-сообщество: Наличие онлайн-сообществ в играх может сделать их привлекательным местом для социального взаимодействия.

• Побег от реальных проблем: Игры могут стать способом побега от реальных проблем и стресса.

• Химический эффект: Некоторые видеоигры стимулируют выработку химических веществ в мозге, вызывая зависимость.

• Игровая привлекательность: Некоторые игры разрабатываются с учетом психологических аспектов, делая их привлекательными и заставляя игрока возвращаться.

Зависимость от новостей относится к необычно интенсивному и частому потреблению новостей в интернете, телевидении или других медийных источниках. Люди, страдающие от этого вида зависимости, могут постоянно проверять новостные сайты, обновлять свои новостные ленты в социальных сетях и быть постоянно в курсе текущих событий. Это может привести к постоянному напряжению, тревоге и чувству беспокойства, особенно если новости часто негативны.

Признаки зависимости от новостей:

• Постоянное обновление новостных источников: Зависимые от новостей могут постоянно обновлять новостные сайты, приложения и социальные медиа, чтобы быть в курсе последних событий.

• Отсутствие контроля: Люди могут терять контроль над временем, проведенным на чтение новостей, что может отрицательно сказаться на повседневных обязанностях.

• Переживание избытка тревожной информации: Зависимые могут испытывать избыток тревожной информации, что приводит к чувству беспокойства и бессонницы.

• Изменения в настроении: Новости, особенно негативные события, могут влиять на эмоциональное состояние, вызывая уста-

лость, раздражение и депрессию.

• Изоляция: Постоянное внимание к новостям может привести к изоляции от социальных событий и важных моментов в реальной жизни.

• Сравнение себя с другими: Люди могут начать сравнивать свою жизнь и проблемы с проблемами других, что может вызвать чувство неудовлетворенности.

Причины появления зависимости от новостей могут включать в себя:

• Беспокойство и тревога: Новости часто содержат информацию о проблемах и кризисах, что может поддерживать чувства беспокойства.

• Потребность в контроле: Зависимость от новостей может быть связана с потребностью в контроле над окружающим миром.

• Социальное давление: Общественное давление следить за новостями может подталкивать людей к постоянному вниманию к новостным событиям.

• Поиск информации о собственной безопасности: Временами люди могут поглощаться новостями из-за потребности в информации о своей собственной безопасности и благополучии.

Думскроллинг (от английского doom — «гибель, судьба, рок, Судный день» и scrolling — «прокрутка») - это термин, который описывает поведение людей, которые постоянно прокручивают новости в поисках негативных, тревожных или страшных событий, несмотря на то что они огорчают и деморализуют человека. Это поведение может привести к чрезмерной тревожности и стрессу. Вместо того чтобы остановиться, когда человек сталкивается с негативной информацией, он продолжает прокручивать новости, погружаясь в «душный» поток негативных событий.

Зависимость от новостей и дум скролинга могут оказывать отрицательное воздействие на психическое здоровье, вызывая тревогу, беспокойство и ухудшение эмоционального состояния. Важно находить баланс в потреблении новостей, осознанно выбирая и ограничивая время, проведенное в новостных источниках, чтобы поддерживать психологическое благополучие.

Зависимость от социальных сетей — это состояние, при котором человек испытывает патологическую потребность в постоянном использовании социальных медиа, таких как вКонтакте, одноклассники, TikTok и других. Эта зависимость может оказывать негативное воздействие на физическое и психическое здо-

ровье, а также на социальные взаимоотношения.

Признаки зависимости от социальных сетей:

• Чрезмерное время, проводимое в социальных сетях: Зависимые от соцсетей часто тратят неоправданно много времени на просмотр ленты, комментирование и поиск контента.

• Отсутствие контроля: Люди могут не иметь контроля над своим временем в социальных сетях, игнорируя другие важные обязанности.

• Неконтролируемое обновление: Постоянное обновление своего профиля, поиск лайков и комментариев становятся приоритетными действиями.

• Изменения в настроении: Реакции на активность в соцсетях могут влиять на эмоциональное состояние, вызывая радость от положительных откликов и стресс от отрицательных.

• Сравнение себя с другими: Зависимые часто сравнивают свою жизнь и успехи с жизнью других, что может вызвать чувство неудовлетворенности и зависти.

• Изоляция: Зависимость от социальных сетей может привести к уходу от реальных социальных взаимодействий, создавая иллюзию общения через экран.

Причины появления зависимости от социальных сетей могут включать в себя:

• Потребность в подтверждении: Люди могут искать подтверждение своей личности и успехов через лайки и комментарии в соцсетях.

• Страх пропустить что-то важное: Социальные сети часто представляют собой источник новостей и событий, и люди могут бояться упустить что-то важное, поэтому постоянно следят за обновлениями.

• Психологическая награда: Получение лайков и положительных комментариев может вызывать у человека ощущение удовлетворения и радости, действуя как психологическая награда.

• Механизм борьбы со стрессом: Для многих людей социальные сети становятся способом справиться со стрессом и уходом от реальных проблем.

Важно находить баланс в использовании социальных сетей и уделять внимание реальным жизненным аспектам. При наличии признаков зависимости может быть полезно обратиться за профессиональной помощью и осознанно управлять временем, проводимым в онлайне.

Зависимость от смартфонов — это патологическое состояние, при котором человек испытывает навязчивую и чрезмерную потребность использовать смартфон, что может сказываться на его физическом и психическом здоровье, а также социальных отношениях. Эта зависимость может включать в себя постоянное использование телефона для общения в социальных сетях, чтения новостей, игр, просмотра видео и других действий, влияющих на повседневную жизнь человека.

Признаки зависимости от смартфонов:

• Чрезмерное использование: Человек проводит чрезмерно много времени, используя смартфон, иногда непрерывно и даже ночью.

• Снижение производительности: Зависимость от смартфонов может привести к снижению производительности на работе или в учебе из-за отсутствия фокуса.

• Отказ от реальных обязанностей: Постепенный отказ от выполнения реальных обязанностей в пользу времени, проведенного в онлайн-активностях.

• Физические проблемы: Долгие периоды использования смартфона могут вызывать физические проблемы, такие как напряжение в шее, спине и глазах.

• Изоляция: Использование смартфона может привести к изоляции от реальных социальных взаимодействий, влияя на отношения с окружающими.

• Страх пропустить информацию: Постоянный страх пропустить важные события, новости или сообщения, что становится приоритетом перед реальной жизнью.

Причины появления зависимости от смартфонов могут включать в себя:

• Социальное давление: Потребность соответствовать социальным трендам и быть всегда в курсе новостей.

• Психологическая удовлетворенность: Использование смартфона может приносить психологическую удовлетворенность и уклонение от реальных проблем.

• Интернет-развлечения: Легкий доступ к разнообразным формам онлайн-развлечений, таким как игры, социальные сети и видео.

• Общественное признание: Популярность и успешность в онлайн-среде могут стать стимулом для постоянного использования смартфона.

• Скука: Недостаток занятий или долгие периоды скуки могут способствовать зависимости от смартфона.

Лечение зависимости от смартфонов может включать в себя осознанное управление временем, установку границ использова-

ния устройства, поиск альтернативных развлечений и, при необходимости, профессиональную помощь.

ОБЩИЕ ПРИЗНАКИ ЦИФРОВОЙ ЗАВИСИМОСТИ

Хотя каждая из указанных зависимостей (цифровая, от социальных сетей, от новостей, игровая, от смартфонов) имеет свои особенности, существуют некоторые общие признаки, которые могут свидетельствовать о возможной проблеме зависимости:

• Чрезмерное время. Зависимость часто проявляется в чрезмерном времени, уходящем на занятия зависимым поведением. Это может быть бесконечный прокрут новостной ленты, часы проведенные в социальных сетях, игры без остановки или постоянное использование смартфона.

• Утрата контроля. Люди с зависимостью теряют способность контролировать своё поведение в отношении использования цифровых технологий. Они могут не соблюдать умеренность и продолжать заниматься зависимым поведением, несмотря на негативные последствия.

• Отказ от реальных обязанностей. Зависимость может привести к уклонению от реальных обязанностей, будь то учеба, работа или личные отношения. Человек может предпочесть виртуальный мир реальной жизни.

• Физические и психические проблемы. Постоянное использование цифровых технологий может вызвать физические проблемы, такие как бессонница, напряжение в глазах, боли в спине, а также психологические проблемы, включая тревогу, депрессию и раздражительность.

• Изменения в поведении и эмоциональном состоянии. Зависимость может сопровождаться изменениями в поведении, такими как изоляция, раздражительность, агрессия или апатия. Эмоциональное состояние человека может зависеть от результатов виртуальных взаимодействий.

• Социальная изоляция. Зависимость часто приводит к социальной изоляции, поскольку человек предпочитает виртуальные взаимодействия реальным. Это может сказываться на отношени-

ях с семьей, друзьями и коллегами.

Обратите внимание, что наличие одного или нескольких этих признаков не всегда означает наличие зависимости. Важно учитывать контекст и степень влияния на общую жизнь человека. Если возникают беспокойство и негативные последствия, обращение за профессиональной помощью может быть полезным.

Способы борьбы с цифровой зависимостью

Борьба с цифровыми зависимостями требует системного подхода и внесения изменений в поведение и образ жизни. Вот несколько стратегий, которые могут помочь в борьбе с различными видами зависимостей:

1. Создание плана. Разработайте конкретный план действий для пошагового преодоления зависимости. Включите в него цели, сроки и конкретные шаги для реализации.

2. Ограничение использования. Определите конкретные временные рамки для использования цифровых технологий. Это может включать в себя установку ограничений на время игры, чтения новостей или просмотра социальных сетей.

3. Цифровой детокс. Регулярно проводите периоды цифрового детокса, в течение которых вы полностью отказываетесь от цифровых устройств. Это может помочь восстановить баланс и освежить ум.

4. Поиск альтернатив. Найдите заменяющие занятия, которые приносят радость и удовлетворение. Это может быть занятие спортом, чтение книг, рисование, музыкальные занятия или другие хобби.

5. Социальная поддержка. Обсудите свои проблемы с близкими людьми. Поддержка друзей и семьи может быть важной частью преодоления зависимости.

6. Управление стрессом. Определите и используйте стратегии для эффективного управления стрессом. Это может включать в себя практику релаксации, медитацию или дополнительную физическую активность.

7. Развивайте навыки управления временем. Обучитесь эффек-

тивному управлению временем, чтобы обеспечить баланс между цифровыми активностями и другими аспектами вашей жизни.

8. Осознанное использование цифровых устройств. Будьте осознанными в отношении своего использования цифровых устройств. Сделайте паузы для размышлений о том, как вы проводите время в виртуальном мире и как это влияет на вашу реальную жизнь.

9. Обучение цифровой грамотности. Развивайте навыки цифровой грамотности, чтобы эффективнее управлять своим онлайн-присутствием и использованием цифровых технологий.

10. Профессиональная помощь. Если зависимость серьезна и влияет на вашу жизнь, обратитесь за профессиональной помощью. Психотерапевты и консультанты могут помочь вам понять корни проблемы и разработать стратегии преодоления зависимости.

Важно помнить, что каждый человек уникален, и подход к преодолению зависимости может потребовать индивидуального подхода. Если вы сталкиваетесь с серьезными трудностями, обращение за помощью у профессионала может быть полезным шагом.

Учебно-методическое пособие по формированию культуры безопасности

Руководитель проекта - Юрий Пивненко,
председатель Санкт-Петербургского регионального
отделения Российского Союза Спасателей.

Автор Станислав Боголепов

Редактор Анастасия Панкина

РАСПРОСТРАНЯЕТСЯ БЕСПЛАТНО

2023год