

Безопасность в цифровой среде

Понятие – «цифровая среда»

Для современной молодёжи компьютер, смартфон или планшет стали неотъемлемой частью повседневной жизни, а предоставляемый ими доступ к информации и общению – абсолютно естественным явлением.

Однако эти и другие устройства, а также формируемое с их помощью пространство человеческих взаимодействий и распространение информации создают принципиально новое измерение существования – **цифровую среду**.

Цифровая среда – пространство взаимодействия людей между собой или людей с электронными сервисами. Доступ в это пространство осуществляется с помощью электронных устройств и программного обеспечения.

К этим взаимодействиям относятся поиск и получение информации; отправка и приём сообщений; публикация информации (текстовой, графической, видео- или аудиоинформации).

В этих взаимодействиях человек выступает и как потребитель контента цифровой среды, и как его создатель.

Улучшая и упрощая повседневную жизнь, обеспечивая простой и быстрый доступ практически к любой информации, ускоряя человеческое общение, цифровая среда имеет и отрицательную сторону. Прежде всего это:

- ▶ иллюзия защищённости;
- ▶ иллюзия приватности;
- ▶ иллюзия анонимности;
- ▶ иллюзия доверительности.

Именно эти иллюзии делают пользователя особенно подверженным рискам, которые несёт в себе цифровая среда. Чем вызваны эти иллюзии, как на самом деле работает тот или иной аспект цифровой среды, мы рассмотрим в следующих темах, посвящённых информационным рискам и угрозам. Однако главный отличительный признак цифровой среды нужно сформулировать уже сейчас.

!!! Весь контент, загружаемый пользователями в цифровую среду, хранится вечно и в любой момент доступен для обнаружения, исследования, обработки и, как следствие, применения третьими лицами.

Пользователи в интернете при взаимодействии друг с другом или с электронными сервисами создают и передают информацию, которая сохраняется на различных устройствах: компьютерах, смартфонах, серверах интернет-провайдеров, сетевом оборудовании и т.п. Другими словами, активность в Сети оставляет **цифровые следы** – «отпечатки» деятельности и личности пользователя. С помощью цифрового следа можно не только установить личность пользователя, но и узнать многое о его жизни и привычках.

Цифровая следы

В цифровой среде ничто не остаётся незамеченным, ни одно действие не может быть совершено скрытно: абсолютно все действия человека в этой среде фиксируются и могут быть исследованы.

Человек оставляет цифровые следы:

- ▶ **в устройстве**, которое использует в цифровой среде (будь то компьютер, смартфон или планшет): время и интенсивность использования устройства; геопозиция; введенные тексты; использованные программы и приложения; используемые контакты из телефонной книги; в пассивном режиме работает микрофон, а нередко и ведётся запись со встроенной камеры. Смартфоны и смарт-часы, помимо этого, сохраняют показатели вашей физической активности и все маршруты ваших перемещений;
- ▶ **на посещённых сайтах**: информация о том, где вы находитесь, что привлекло ваше внимание, сколько времени вы уделили чтению (и что именно вы читали на сайте, и как именно вы читали – внимательно или нет), какие страницы вы посещали до этого;
- ▶ **в поисковых машинах**: информация о том, что и когда вы искали, какими результатами поиска воспользовались, на какие сайты перешли;
- ▶ **Wi-Fi-роутере**: время выхода в Интернет, посещённые сайты и объём использованного вами трафика.

Кроме того:

- ▶ если телефон **выключен**, он всё равно постоянно определяет ваше местоположение: и по вышкам сотовой связи, и с помощью общедоступных беспроводных сетей **Wi-Fi**;
- ▶ если у человека **нет цифровых устройств**, но он передвигается по городу, в транспорте, заходит в учреждения, офисы, пользуется банкоматом и т.д., его постоянно фиксируют видеокамеры.

Компании Google и Apple (и их бизнес-партнёры) отслеживают:

- ▶ местоположение десятков миллионов пользователей с точностью до 50 метров в любой момент времени, и их перемещения, привычные маршруты и многое другое;
- ▶ периоды активности, социальный статус, все фотографии на устройствах;
- ▶ все персональные данные пользователей (личные, банковские), переписки по SMS и электронной почте, профессию и т.д.

Цифровые следы в социальных сетях

Особое внимание необходимо обратить на цифровые следы, которые мы оставляем в социальных сетях, а именно:

- ▶ добровольно предоставленные пользователями массивы информации о себе, родных и близких: возраст, адрес, материальное положение, увлечения и привычки, фотографии и видеоролики и др.;
- ▶ собранные социальными сетями данные с помощью программного обеспечения без информирования пользователя.

Пользователям кажется, что социальная сеть создана для общения, но **цель владельцев социальной сети** – получение прибыли путём коммерциализации (монетизации) собираемых платформой разнообразных данных пользователей. Поэтому любая социальная сеть проектируется так, чтобы мотивировать пользователя на длительное пребывание и размещение как можно большего количества информации.

Социальные сети и иные наблюдатели постоянно анализируют весь контент, который вы разместили, причём не только текстовый (фотографии и видео способны предоставить очень много сведений о пользователе). При этом социальные сети знают не только то, что пользователь разместил в их пределах (на множестве обычных сайтов,

приложений установлены специальные **коды** социальных сетей). Коды социальных сетей призваны максимально упростить пользование сайтом. Например:

- ▶ единые формы авторизации через социальные сети;
- ▶ модули комментирования, при помощи которых можно опубликовать своё мнение о материале, не покидая сайт;
- ▶ инструменты «социализации», при помощи которых можно лайкнуть или «расшарить» материал, не покидая сайт, на котором он опубликован;
- ▶ **следающие пиксели**, при помощи которых владелец сайта может изучать эффективность рекламы и получать точную статистику пользователей.

Но одновременно с этим такие коды собирают информацию и о ваших действиях, формируя детальную картину вашего сетевого поведения.

***Следающие пиксели** – невидимые файлы изображений, внедряемые в контент страницы, электронного письма. Размер такого изображения обычно равен 1х1 пиксель (пиксель – минимальный элемент изображения на экране). При загрузке страницы сайта или письма следающие пиксели передают на сервер владельца сайта информацию об устройстве пользователя и просмотре информации. Предотвратить действия следающих пикселей можно, запретив автоматическую загрузку изображений в веб-браузере или включив блокировку переходов по ссылкам.*

Накопление огромных массивов данных о пользователях приводит к тому, что сам пользователь постоянно подвергается риску утечки данных о нём. Ведь к собранным таким образом сведениям имеют доступ очень многие производители мобильных устройств, операторы мобильной связи, интернет-провайдеры, администрация торговых центров, сотрудники правоохранительных органов и др. Многими из этих данных могут без особых трудов завладеть и злоумышленники. Это влечёт за собой опасность кражи финансовых средств, оформления на пользователя кредита, шантажа и т.д.

Существует ли приватность в Интернете?

Учитывая, что любая активность в Интернете оставляет цифровые следы, можно утверждать, что приватность в Интернете – миф: любая информация, которая однажды попала в Интернет, может быть там найдена. Это лишь вопрос желания и ресурсов, которые кто-то готов на это затратить. Как уже отмечалось ранее, и наши мобильные устройства, и внешние наблюдатели знают о нас очень много.

Персональные данные граждан, в том числе и в цифровой среде, защищаются Федеральным законом от 27 июля 2006 г. № 152-ФЗ (в последней редакции) «О персональных данных».

*Понятие **персональных данных** определяется как «любая информация, относящаяся прямо или косвенно к определённому лицу». Это определение позволяет относить к персональным данным практически любую информацию – фамилию, имя, отчество и дату рождения; сведения о семейном положении и образовании; адрес проживания; телефонный номер и адрес электронной почты и многое другое. Изображения, по которым можно установить личность, также относятся к персональным данным.*

Большую часть персональных данных пользователь сам охотно предоставляет в Интернете – публикует в социальных сетях, отправляет в мессенджерах. Для того, чтобы завладеть этими данными, не требуется хакерских ухищрений, ведь они добровольно выложены в Интернет самими пользователями.

Виды цифровых рисков

Цифровая среда не только усугубляет опасность существовавших ранее рисков, но и формирует принципиально новые

Риски цифровой среды можно разделить на две большие группы:

- ▶ **информационные** (угроза сознанию и здоровью пользователя);
- ▶ **электронные** (угроза нанесения ущерба устройствам, приложениям, данным; хищения финансовых средств или данных).

Информационные риски связаны с:

- ▶ опасным контентом и неприемлемым поведением (например, травля). Эти риски существовали и прежде, но возросшая скорость распространения информации и психологические особенности сетевого поведения (ощущение безнаказанности, анонимности, восприятие действий в Интернете как ненастоящих) значительно увеличили их опасность;
- ▶ вовлечением в деструктивное поведение: появление вербовщиков, предлагающих пользователям деструктивный контент в привлекательной упаковке; возможность создания сообществ, почти не оставляющих пользователю шанса вырваться из информационной ловушки;
- ▶ недостоверными сведениями, которые создаются в погоне за трафиком и быстро распространяются среди массовой аудитории Интернета.

Цифровая среда не только добавляет новое измерение в уже существующие риски. Уникальная специфика цифровой среды и появление новых возможностей порождают и принципиально новые **электронные риски**. Доступность информации, лёгкость скорость информационного обмена имеют свою «тёмную сторону» - то, что составляет основную ценность цифровой среды, одновременно делает пользователя уязвимым.

К ним относятся:

- ▶ кража персональной информации, которая может быть использована для нанесения ущерба пользователю;
- ▶ заражение компьютерным вирусом, которое осложнит (или сделает невозможным) пользование устройством или приведёт к потере данных;
- ▶ проникновение вредоносных программ, использующих ресурсы устройства пользователя для достижения целей третьих лиц (это может быть майнинг криптовалют, показ огромного количества нежелательной рекламы).

***Криптовалюта** – это цифровые «псевдоденьги», существующие только в цифровом виде, никак не выражаемые материально. Добывают криптовалюту при помощи производства на пользовательских устройствах сложных ресурсоёмких вычислений – этот процесс называется майнингом: он сильно изнашивает компоненты устройства и требует много электроэнергии. Никакого практического значения эти вычисления не имеют и пользы не приносят. Называть криптовалюту деньгами неверно – в отличие от денег она не обеспечена никакими активами, её ценность не зависит от государства. Курсы криптовалют зависят исключительно от новостей рынка криптовалют, распространяемых слухов и манипуляций на информационном поле.*

Одними из основных **источников рисков** являются:

- ▶ иллюзия анонимности и приватности в Интернете;
- ▶ высокий уровень доверия к получаемой информации, неумение распознать угрозу;
- ▶ недостаток знаний о цифровой гигиене и рисках.

Цифровая зависимость

Цифровая зависимость является ещё одной крайне специфической опасностью, порождённой цифровой средой. Суть этой зависимости – постоянная потребность погружения в эту среду. В первую очередь она проявляется в предпочтении гаджетов общению с людьми в повседневной деятельности. Проще говоря, если человек предпочитает общаться со смартфоном или компьютером, а не с друзьями, вместо домашних и рабочих дел или учёбы сидеть в Интернете – у него налицо цифровая зависимость.

Как и любая другая зависимость, цифровая часто не осознаётся самим пользователем, который принимает её за норму современной жизни.

Признаками **цифровой зависимости** являются:

- ▶ постоянное увеличение количества времени, проводимого за устройством (компьютером, смартфоном или иным гаджетом);
- ▶ частый бессистемный просмотр информации в Интернете;
- ▶ ухудшение эмоционального состояния при ограничении доступа в Интернет;
- ▶ длительное (многочасовое) «зависание» в компьютерных играх или на интернет-площадках;
- ▶ навязчивое стремление обновлять ленту (постоянное чтение новостей или социальных сетей);
- ▶ стремление любой ценой получить доступ к игре или в Интернет.

Последствия цифровой зависимости:

- ▶ нарушение ритма жизни – цифровая активность отнимает значимую часть времени;
- ▶ психологическая нестабильность (вплоть до развития депрессии);
- ▶ повышенные раздражительность и агрессивность;
- ▶ ухудшение физического состояния – от пониженного общего тонуса до опасных для здоровья колебаний веса.

Необходимо понимать, что платформы в цифровой среде (социальные медиа, новостные сайты и т.д.) устроены так, чтобы заставить пользователя как можно больше времени проводить на них. Помните, что их цель – коммерциализация (монетизация), а вот механизмы и алгоритмы её достижения настроены таким образом, чтобы способствовать развитию цифровой зависимости пользователя.

*Отдельной разновидностью цифровой зависимости является зависимость от видеоигр, или **игровое расстройство**, - оно выражается в навязчивом желании играть в компьютерные игры. Игровое расстройство включено в новую редакцию Международной классификации болезней (МКБ).*

Как можно избежать этой опасности?

- Установить лимит времени на компьютерные игры и соблюдать его.
- Уделить достаточное время общению с родными и друзьями, занятиям спортом, ремёслами и искусством, прогулкам и туризму.

Литература:

Основы безопасности жизнедеятельности: базовый уровень: учебное пособие для образовательных организаций, реализующих образовательные программы среднего профессионального образования: в 2 частях/ под ред. Ю.С.Шойгу. – Москва: Просвещение, 2024. – (Учебник СПО).

Ч.2. Модуль 8. Безопасность в информационном пространстве. Тема 1. Безопасность в цифровой среде. с 108.