«Основы безопасной работы в сети Интернет»

Модуль 1. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами

Информационная среда и политика информационной безопасности

Современный мир характеризуется стремительным развитием цифровых технологий. Происходит цифровизация общества, т.е. цифровые технологии внедряются в различные виды деятельности человека.

Люди доверяют компьютеру личную информацию, не зная или не задумываясь о связанных с этим рисках. Персональные данные, которые вы вносите при заполнении профиля в социальной сети или данные онлайн-банкинга – всё это является целью злоумышленников, поэтому каждый пользователь может стать потенциальной жертвой.

В этих условиях на первый план выходит вопрос обеспечения информационной безопасности, т.е. обеспечения конфиденциальности, целостности и доступности информации. Задачи обеспечения информационной безопасности:

1. Обеспечение права личности и общества на получение информации.

2. Обеспечение объективной информацией.

3. Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.

4. Защита личности, организации, общества и государства от информационно-психологических угроз.

5. Формирование имиджа, борьба с клеветой, слухами, дезинформацией.

В социальном плане информационная безопасность предполагает борьбу с информационным «загрязнением» окружающей среды, использованием информации в противоправных и аморальных целях.

Фейковые новости: чем опасны, как отличить и чему верить?

Фейковые (фальшивые) новости – дезинформация для получения выгоды:

Деньги – привлечь трафик, заработать на рекламе.

Слава – привлечь внимание, стать знаменитым.

Политика – повлиять на общественное мнение.

Конкуренция – повлиять на репутацию или стоимость акций.

Способы распространения: социальные сети, развлекательные сайты, желтая пресса, блоги.

Как можно защититься от фальшивой информации?

Не доверять громким заголовкам. Фейковые новости с самого заголовка буквально кричат о своей важности и исключительности. Желательно с восклицательным знаком в конце. Поэтому если заголовок кажется вам невероятным, то вероятно, что это выдумка журналиста.

Проверять источник информации: откуда статья, кто автор? Убедитесь, что читаете именно то издание, которому вы доверяете. Если материал опубликован в никому не известном издании, то перед тем, как пересказывать кому-то прочитанную новость, попробуйте побольше о нём узнать. Как правило на любом приличном сайте есть вкладки вроде «О нас».

Следите за опечатками. Часто фейковые новости грешат большим количеством ошибок и опечаток.

Не доверять авторским оценкам: Важны факты! Если это серьезный текст, но автор не удосужился расставить ссылки на первоисточники, приводит исследования неназванных экспертов, то это либо осознанный фейк, либо фантазии автора, которые он пытается выдать за факты.

Подписаться на надежные источники новостей. Поищите эту новость в других изданиях. Если ее нет больше нигде, то, скорее всего, эта новость ложная. Если же об этом написали авторитетные сайты, которым вы доверяете, то новость, скорее всего настоящая.

Обратите внимание на дату публикации. Многие фейковые новости никак не датированы, потому что говорят о событиях, которых никогда не было.

Противодействие идеологии терроризма в сети Интернет

Интернет широко используется террористическими группировками для пропаганды своих идей. Такие акции ориентированы, прежде всего, на молодежь, поскольку именно она является наиболее восприимчивой и легко может поддаться течению той или иной идеологии. Также в сами экстремистские группировки входят чаще всего молодые специалисты, которые владеют различными навыками, хакерскими способностями. В таких социальных сетях, как «Вконтакте», «Facebook», «Одноклассники» террористы могут найти своих сторонников через опросы различного характера, по которым они смогут определить отношение человека к той или иной проблеме. Для противодействия этой деятельности в России открыто множество сайтов, занимающихся борьбой с идеологией терроризма и экстремизма. Например, «Наука и образование против террора» (http://scienceport.ru/), «Молодежь за Чистый Интернет» (http://www.honestnet.ru/) и множество других ресурсов. Интернет-ресурсы играют очень важную роль в организации антитеррористической пропаганды, воспитания в людях неприятия идеологии терроризма и экстремизма.

Какие материалы не стоит размещать у себя на странице

Информационная безопасность предполагает соблюдение определенных правил при общении в социальных сетях. Ни в коем случае не стоит размещать у себя на странице информацию следующего плана:

Риторика ненависти

Публичное выражение ненависти, оскорбление (хейтспич) в адрес любой группы людей оскорбляет ваших читателей, выставляет вас в невыгодном свете и может быть основанием для возбуждения уголовного дела по статье 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства». В комментариях к подобным постам других пользователей тоже лучше не появляться, а вот пожаловаться на публикацию можно и даже желательно.

Клевета

Прежде чем публиковать заведомо ложную информацию о другом человеке, чтобы «насолить» ему, вспомните о том, что в нашей стране клевета уголовно наказуема (статья 128.1 УК РФ). То же самое касается репостов обличительных записей, в правдивости которых вы не уверены.

Пропаганда запрещенных веществ

Конечно, никто не может вам запретить шутить в социальных сетях на тему психоактивных веществ, но будьте готовы к повышенному вниманию со стороны правоохранительных органов. Закон «О защите детей от информации, причиняющей вред их здоровью и развитию» запрещает публиковать любую информацию о способах изготовления и употребления психоактивных веществ. То же касается методов совершения суицида и любых упоминаний детской порнографии.

Экстремистские высказывания и призывы к массовым беспорядкам

Шутки на тему захвата Кремля компанией друзей в пятницу вечером или выделения Гольяново в отдельное государство могут обернуться уголовным преследованием по 280 и 212 статьям УК РФ. Особенно если пост будет размещен в публичном доступе. Поэтому вместо таких шуток лучше котика запостите.

Если вы встретили в сети Интернет запрещенную информацию, необходимо сообщить об этом в соответствующие организации для дальнейшей блокировки данных ресурсов. Такую возможность предоставляет сайт «Медиа Гвардия» (http://mediagvardia.ru/). Это федеральный проект, целью которого является объединение усилий интернет-пользователей для совместного выявления интернет-сайтов, сообществ и групп в социальных сетях, специализирующихся на распространении противоправного контента.

В России создан «Реестр запрещённых сайтов» для борьбы с наркотиками, детской порнографией и пропагандой суицида в сети Интернет. Действуют федеральные законы, которые запрещают распространение материалов экстремистского и террористического характера. Закрыты тысячи сайтов, но если сейчас забить в поисковике любое из этих направлений, то можно найти необходимые ресурсы, не говоря о тех, которые закрыты для индексации. На сайте «Медиа Гвардия» предлагается всего несколькими кликами сделать интернет чище и безопасней. Для этого необходимо зарегистрироваться на сайте и присылать обращения, если Вы столкнулись в сети Интернет с запрещенной информацией.

Важным аспектом обеспечения информационной безопасности является безопасность финансовых операций. При всех очевидных плюсах электронных платежей совершенно не всегда финансовые операции онлайн безопасны. Для обеспечения безопасности электронных денег очень важно пользоваться лицензионными антивирусами, осторожно пользоваться публичными сетями, не вводить пароли на чужих компьютерах, не записывать и не хранить пароли онлайн.

Тему безопасности электронных платежей мы с вами более подробно рассмотрим в модуле 4 «Меры предосторожности при проведении Интернет-транзакций», а сейчас перейдем к вопросам защиты от компьютерных вирусов.

Модуль 2. Компьютерная безопасность и Интернет-безопасность

Виды компьютерных угроз. Возможные риски и предотвращение угроз.

Компьютерная безопасность считается одним из направлений информационной безопасности в целом, т.к. информационная безопасность подразумевает защиту не только на аппаратном уровне. Т.е. говоря о компьютерной безопасности, мы можем оперировать более общим термином «информационная безопасность».

Угрозы информационной безопасности

Угрозы информационной (компьютерной) безопасности – это действия, которые могут нанести ущерб информационным и компьютерным системам. Угрозы могут быть преднамеренные и непреднамеренные. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, которые не входят в число необходимых для работы, в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников, но к домашним компьютерам это отношения практически не имеет.

Классификация угроз информационной безопасности

В зависимости от различных способов классификации существуют различные угрозы информационной безопасности:

a) Нежелательный контент
b) Несанкционированный доступ
c) Потеря данных
d) Мошенничество

Нежелательный контент – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные компьютерные вирусы, шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством. В современном мире интернетом пользуются люди разных возрастов, будь то ребенок или пожилой человек, каждый имеет страницу в социальной сети, пользуется поисковыми системами для получения ответов на вопросы, смотрит видео, читает книги или слушает музыку. В связи с этим вероятность того, что пользователь встретит в сети нежелательный контент, очень велика, и от вида контента будет зависеть размер полученного ущерба.

Классификация нежелательного контента

Вредоносное программное обеспечение или какой-либо другой нежелательный контент может попасть в компьютер с файлом, скачанным из интернета, либо после перехода по сторонней ссылке или путем рассылки спама и т.д. Поэтому весь нежелательный контент можно разделить на несколько основных типов:

1) Вредоносные программы
2) Спам
3) Потенциально опасные программы
4) Запрещенные законодательством сайты
5) Нежелательные сайты

К первому типу можно отнести компьютерные вредоносные программы, которые внедряются в программы, установленные на ПК, без согласия пользователя. Вредоносные программы отличаются между собой методами заражения и типами объектов, которые они заражают. Подцепить вредоносную программу можно разными способами, например, на вредоносном сайте или из неизвестного письма, скачав файл или перейдя по ссылке. Вредоносная программа имеет множество задач, основная часть которых направлена на нанесение вреда ОС. Сетевые черви тоже относятся к этому типу, они похожи на компьютерные вредоносные программы. Главное отличие в том, что черви не заражают

существующие файлы, а хранятся отдельными файлами, и распространяются посредством уязвимостей Сети и ОС. Также к этому типу относятся приложения, выполняющие задачи злоумышленников, скрываясь под видом законного приложения (трояны), и вредоносные программы, скрывающие свое присутствие не только от пользователя, но и от защитного ПО (руткиты). Не менее опасными являются бэкдоры, которые позволяют злоумышленнику не только управлять любым приложением на ПК, но и производить запись видео/аудио с имеющейся камеры/микрофона, загружать и сохранять файлы, сохранять последовательности нажатия клавиш.

Спам – это письма, которые приходят на электронную почту от неизвестных людей и компаний. Такие письма обычно имеют завлекающую тему и содержат какую-либо рекламную информацию, призывающую что-то купить или выиграть. Выполняя действия, описанные в письме, можно потерять не только деньги, но и путем просмотра прикрепленных к письму документов и картинок, загрузить вредоносную программу на свой компьютер, что может привести к потере личной информации.

К потенциально опасным программам можно отнести программы, которое содержит рекламу (adware), и шпионские программы (spyware), скрытно устанавливаемые на устройство без согласия пользователя, с целью сбора информации или изменения каких-либо настроек.

Каждый сам решает, какая информация для него является нежелательной, что загружать на свой ПК, какие сайты посещать, при этом, в некоторых моментах осознанно идя на риск. Но есть сайты, запрещенные законодательством, то есть существует единый реестр запрещенных сайтов, в который занесены сайты, содержащие информацию, распространение которой запрещено в Российской Федерации.

Для различных возрастных категорий существуют свои нежелательные сайты, которые могут содержать информацию, не соответствующую возрасту пользователя компьютера. Также к этому типу можно отнести сайты, блокируемые на рабочих местах, с целью уменьшения траты времени работниками на развлечения.

Объект воздействия

Угрозе заражения подвержены домашние и корпоративные пользователи, владельцы смартфонов и персональных компьютеров, все устройства имеющие подключения к интернету. Никто на 100% не защищен от вредоносных программ, но неопытные пользователи более уязвимы. Если человек знает, что такое вредоносное ПО и как оно может попасть в компьютер, то злоумышленнику придется постараться, чтобы добраться до жертвы. А, если пользователь не знаком с подобными терминами, то он становится легкой добычей для атакующего. Если пользователь имеет опыт работы с

различными приложениями, то он не будет скачивать на свой ПК сомнительные файлы или посещать сайты такого же характера. Это и отличает опытного пользователя от неопытного, последний не раздумывая, будет кликать и загружать. То же касается и спам рассылок, опытный пользователь знает, к чему приводят подобные сообщения, не будет переходить по ссылкам, загружать прикрепленные документы, заполнять какие-то анкеты, переводить куда-то деньги и прочее. Подобного рода спам рассчитан на детей и наивных, падких к легкой добыче людей, которые увидев громкий заголовок или яркую картинку, без сомнения перейдут по ссылке.

Источник угрозы

Основным генератором вредоносных программ является киберкриминальный бизнес. Киберпреступники зарабатывают деньги на нежелеательном контенте. Вредоносные программы представляют собой самовоспроизводящийся программный код, который содержит определенные алгоритмы выбора объектов и методов заражения. Трояны, бэкдоры, руткиты и шпионские программы посредством своей скрытности незаметно для пользователя выполняют свои задачи.

Анализ риска

От выше перечисленных угроз помогают защититься комплексные антивирусные средства. Данное ПО работает на основе баз, которые постоянно обновляются, что позволяет обнаруживать новые виды угроз. Необходимо помнить, что само наличие антивирусной защиты не сможет предотвратить заражение компьютерной системы, если пользователь не будет соблюдать правила безопасности. Для этого пользователь должен обладать знаниями об основных механизмах работы вредоносного ПО.

Для защиты от спам-рассылок используют антиспам-фильтрацию и черные списки. Эти способы доступные и позволяют, если не полностью ограничить себя от спама, то значительно его уменьшить. Чтобы избавиться от большого количества рекламы в браузерах, можно использовать соответствующие расширения, а защитить компьютер от adware программ, которые требуют установку, можно с помощью антивирусных продуктов, имеющих в своем ассортименте функцию «песочница». Это позволит запустить программу в ограниченной среде и не опасаться за безопасность ОС. Для защиты от шпионских программ нужно использовать антивирусы.

Определение степени доверия сайта

Когда большинство источников информации и услуг, включая государственные, размещены в сети Интернет, встает вопрос о способах определения степени доверия к сайтам. Нередки случаи, когда страницы создаются мошенниками для выманивания

денежных средств или персональных данных пользователей. В связи с этим возникла потребность в определении уровня доверия к сайту. Мошеннические сайты очень часто:

- Гарантируют большой денежный выигрыш, но для этого нужно лишь подтвердить личность отправкой смс.
- Имитируют интерфейс знакомых социальных сетей, например, Одноклассников, из-за чего пользователи без задней мысли могут отдать мошенникам свои учетные данные.
- Якобы информационные сайты, имитация форумов и многие другие сайты.

Для определения степени доверия к сайту изначально необходимо убедиться, что Вы переходите именно на нужный ресурс. Это достигается через:

ввод URL-адреса в адресную строку вручную;

переход на сайт через поисковой запрос в поисковой системе.

Кроме того, переход может осуществляться по ссылкам из социальных сетей и писем электронной почты, гиперссылкам из статей. В таком случае необходимо убедиться, что ссылка ведет на нужный вам ресурс, а, например, не на фишинговый сайт. Сделать это можно, наведя курсор на гиперссылку, при этом в левом нижнем углу браузера должен появиться URL-адрес страницы, на которую ведет эта гиперссылка.

Например, на портале «Цифровой гражданин Югры», осуществляя переход в раздел "Контакты", наведя курсор на соответствующий блок, в левом нижнем углу появится ссылка указывающая расположение данной страницы: http://eduhmao.ru/kontakty/

В смартфоне или планшете проверить адрес гиперссылки можно нажав и удерживая элемент содержащий гиперссылку до появления контекстного меню, в котором появится ссылка, по которой будет осуществляться переход.

Виды действий в сети Интернет

Определение степени доверия к сайту стоит проводить исходя из целей, с которыми пользователь заходит на конкретный ресурс. От этого же критерия зависят и признаки, по которым можно установить лояльность к сайту. Далее приведены наиболее распространенные действия пользователей в сети Интернет, расположенные в порядке увеличения значимости определения уровня доверия к ресурсу.

Ознакомление с контентом информационных сайтов

Такие сайты требуют от пользователя только критического подхода к восприятию информации. А для ее анализа необходима проверка достоверности с помощью различных источников или поиск первоисточника. С точки зрения безопасности пользовательских данных – это наименее опасные ресурсы.

Загрузка файлов на компьютер

Подобные цели требуют не только определения степени доверия к ресурсу, но и наличия на компьютере антивирусных средств, которые защитят данные и предупредят пользователя в случае попадания на компьютер вредоносного программного обеспечения. Кроме того, в современных антивирусах предусмотрена функция определения подлинности сайта. Если страница является сомнительной, пользователь будет уведомлен об этом.

Скачивая файлы с какого-либо сайта, нужно в первую очередь оценить надежность этого источника. Сделать это можно с помощью соответствующих сервисов в сети Интернет. Помимо этого, некоторые сайты при скачивании уведомляют пользователя о проверке на наличие вирусов в конкретном файле с помощью антивируса.

При попытке найти в интернете бесплатный контент в виде фильма или программного обеспечения пользователи периодически натыкаются на сайты, предлагающие ввести номер мобильного телефона. Выглядит это примерно так: «Напишите номер своего мобильного, вам придет смс с кодом (или ссылкой), подтвердите ее получение ответной смс-кой (или нажмите на ссылку) и будет вам счастье в виде фильма». Объясняется это защитой от «ботов», но на самом деле вполне возможно, что вас подпишут на платную рассылку или спишут определенную сумму со счета телефона, а нужного файла вы так и не увидите. Часто тут же мошенники размещают сообщение якобы от лица другого пользователя, который утверждает, что прошел все требуемые процедуры и уже скачал файл, и ничего страшного не случится, если вы сделаете то же самое. Не верьте!

Чтобы не попасться на удочку мошенников, соблюдайте правило:

НЕ ВВОДИТЕ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА НА СОМНИТЕЛЬНЫХ САЙТАХ!

Заполнение форм, требующих персональные данные пользователя

Подобные действия выполняются, например, при регистрации на сайте или составлении заказа в интернет-магазине. Важно помнить, что если сайт запрашивает персональные данные (ФИО, дату рождения, адрес проживания, паспортные данные и т. д. Полный список персональных данных приведен в Федеральном законе от 27 июля 2006 г. №152-ФЗ "О персональных данных"), владельцы сайта должны уведомить Вас о том, какие действия будут производиться с персональными данными. Для этого на странице, где вносятся персональные данные, должен быть размещен соответствующий запрос на их обработку и политика конфиденциальности данного ресурса, из которой можно узнать, для чего будут использоваться эти данные.

Также перед вводом персональных данных крайне желательно убедиться в наличии https-соединения, т. е. шифрованного соединения, защищающего персональные данные при передаче от пользователя к сайту. Определить наличие такого соединения для конкретной страницы можно по URL-адресу (расположен в верхней части браузера в адресной строке), который должен начинаться с «https://». Также универсальным показателем для определения подлинности сайта, а также наличия https-соединения является значок зеленого замка, расположенный левее адресной строки браузера. В современных версиях браузеров, в адресной строке, у сайтов использующих незашифрованное http-соединение, префикс "http://" не пишется.

Всё это поможет пользователю определить уровень доверия к данному ресурсу и защитить персональные данные от перехвата злоумышленниками и компрометации.

Совершение денежных операций

На сегодняшний день это очень распространенное действие и в то же время, требующее наибольшей осторожности и бдительности со стороны пользователя. Простейшим примером служит оплата покупок в интернет-магазинах.

Признаки, по которым можно установить степень доверия к таким ресурсам, следующие:

- использование владельцами сайта https-соединения;
- наличие политики конфиденциальности (ознакомиться с ней можно при регистрации или входе);
- возможность подачи претензий по мошенническим платежам;
- наличие форм обратной связи с владельцами сайта.

Отсутствие хотя бы одного из этих признаков может свидетельствовать о том, что данная страница является поддельной.

Операции, связанные с онлайн-банкингом

Понятие онлайн-банкинг подразумевает управление денежными средствами, находящимися на счетах в банках, посредством сети Интернет. К такому виду операций стоит предъявлять наибольшие требования по безопасности. К признакам, приведённым в предыдущем пункте, стоит добавить обязательность пользования онлайн-банкингом только с проверенных устройств, на которых установлены антивирусные средства и доступ к которым имеет ограниченный круг лиц. Желательно управлять онлайн-банкингом только со своего устройства. Также со стороны банковского ресурса должна быть предусмотрена возможность подтверждения онлайн-платежа или перевода с помощью одноразовых паролей, или паролей получаемых пользователями через SMS-сообщение (двухфакторная аутентификация).

Дополнительно существует ряд общих признаков, которые можно учитывать при определении степени доверия к любым сайтам. К ним можно отнести:

- качественная и удобная для чтения вёрстка;
- отсутствие нецензурной лексики и грамматических ошибок;
- регулярное обновление информации и уникальность контента;
- отсутствие большого количества навязчивой рекламы;
- формы обратной связи с владельцами сайта, наличие блогов или групп данного ресурса в социальных сетях.

Кроме определения степени доверия к ресурсу пользователь может отследить подлинность той или иной страницы, что поможет избежать фишинговых сайтов или сайтов, загружающих вредоносное ПО. Для этого существуют специализированные ресурсы по проверке подлинности страниц. Такие сайты позволяют определить степень безопасности любой страницы, а также оценить риск покупок на ней. Кроме того, будет отображена информация о возрасте домена, местоположении сервера и наличии сайта в поисковых системах, а также отзывы от других пользователей.

Рекомендации по определению степени доверия к сайтам

- Наличие шифрования при доступе к сайту (https) у ресурсов, работающих с персональными данными или тех, где совершаются денежные операции.
- Политика конфиденциальности для сайтов, где требуется ввод персональных данных.
- Возможность совершения платежей через одноразовые SMS-пароли.
- Наличие контактов и связи с владельцами сайта через формы обратной связи.
- Работающий и регулярно обновляющийся антивирус.
- Проверка страницы через ресурсы по проверке подлинности сайтов.

Для проверки сайта можно использовать систему по адресу https://довериевсети.рф/. Данный сервис покажет уровень доверия пользователей к сайту, информацию о возрасте домена, местоположении и ip сервера. Кроме этого можно ознакомиться с отзывами людей. Все полученные данные позволят самостоятельно сформировать свое мнение о сайте.

Для проверки сайта дополнительно можно использовать определенный набор критериев, которые помогут вам обезопасить себя в Интернете:

Как правило, мошеннические сайты – это ресурсы-однодневки, не содержащие никакой дополнительной информации кроме той, которая должна ввести пользователей в

заблуждение. Поэтому, если вы перешли на такой сайт, проверьте наличие раздела обратной связи. Как правило, на таких сайтах полностью отсутствует раздел, содержащий информацию о контактах, по которым можно связаться с администрацией сайта. Если вы контакты обнаружили, но все равно сомневаетесь в честности сайта, свяжитесь с разработчиками. Не получили в ближайшее время ответа? Сайт можно смело игнорировать.

Мошеннические сайты не существуют долгое время, поэтому можно проверить, как долго живет данный сайт. Для этого можно использовать сайт Технический центр Интернет (http://www.tcinet.ru/whois/). Если ввести название веб-ресурса в поле Whois, то в результатах вы будете видеть подробную информацию о сайте, включая и дату его создания.

Обзор, установка, настройка антивирусных программ

Для проверки сайта можно также использовать специальные расширения для Интернет-браузеров, например, Avast Online Security или Web of Trust (WOT) – это расширения для браузера, которые позволяет быстро узнать репутацию веб-сайта. С их помощью вы будете видеть, стоит ли переходить на запрашиваемый сайт или нет. Если сайт представляет потенциальную угрозу для вашего компьютера, то Web of Trust будет активно уведомлять вас об угрозах безопасности (мошенничество, вредоносное ПО и фишинг), а Avast Online Security вообще ограничит доступ к подозрительному сайту. Расширения доступны бесплатно и не требуют дополнительной установки антивируса на компьютер.

Модуль 3. Навыки безопасной работы в сети Интернет

Безопасная работа с личным кабинетом

В личном кабинете (далее – ЛК) хранятся персональные данные пользователя информационной системы, а иногда и денежные средства на балансе аккаунта, поэтому необходимо уделить пристальное внимание защите вашего ЛК.

Независимо от того, какую информационную систему вы используете, вы можете стать жертвой злоумышленников. Чтобы минимизировать эти риски необходимо соблюдать рекомендации по безопасности и защите данных. Следуйте им, и угрозы взлома будут вам не страшны.

Сложный пароль

Обратите внимание на криптоустойчивость пароля для входа в ЛК. Пароль должен состоять из букв верхнего и нижнего регистра. Также в нем должны присутствовать

цифры и специальные символы. Минимальная длина пароля составляет 6-8 символов. Для создания безопасного пароля вы можете воспользоваться онлайн-генератором паролей.

Если у вас несколько сгенерированных паролей и вам сложно их запомнить, составьте пароль самостоятельно по следующим рекомендациям:

используйте несвязанные слова или фразы. Например: FlowerElectricityWheel;

используйте русские слова в транслите. Например: Hf,jnfYtDjkr, что означает РаботаНеВолк;

используйте спец. символы (!#$;%) — они усложнят подбор вашего пароля;

не используйте в пароле ваше имя, фамилию и дату рождения;

не используйте слова, связанные с вашим логином или E-mail;

кириллические буквы в пароле запрещены.

Пример пароля: ZexbkczDirjkt#1918! , что означает ЯучилсяВшколе№1918!

Такие пароли достаточно сложные: их легко запомнить и сложно подобрать. Для дополнительной безопасности рекомендуется менять пароль раз в шесть месяцев.

Двухфакторная аутентификация

Двухфакторная аутентификация – одна из обязательных процедур для защиты ЛК. Авторизация в ЛК будет происходить в два этапа. После авторизации с помощью пароля необходимо подтвердить вход при помощи кода, который будет отправлен в SMS-сообщении на указанный номер телефона.

Даже если ваш пароль взломают или украдут, второй этап авторизации по телефону обеспечит вашу безопасность.

Уведомление по E-mail при входе в Личный кабинет

При подключении этого средства защиты после каждой авторизации в системе на контактный e-mail будет приходить письмо с информацией о входе в ЛК. Данные уведомления будут полезны, если вы бываете в ЛК крайне редко. Таким образом, вы сможете своевременно отреагировать при взломе или краже пароля и принять меры по устранению угрозы безопасности.

SMS-сервисы

Один из полезных инструментов для управления личным кабинетом – SMS-сервисы. С помощью данного сервиса вы можете подключить SMS-подтверждение входа в ЛК или SMS-подтверждение для восстановления пароля аккаунта.

Восстановление пароля по e-mail

Если вы забыли пароль от ЛК, вы можете отправить письмо с его восстановлением на e-mail, который был указан при регистрации.

Для обеспечения дополнительной безопасности аккаунта, вы можете включить восстановление пароля доступа по SMS. При включенной опции любой запрос на восстановление доступа к аккаунту необходимо будет подтверждать при помощи кода из SMS-сообщения, который будет отправлен на указанный номер телефона.

Для дополнительной безопасности вы можете отключить восстановление пароля по e-mail. В таком случае, если злоумышленники получат доступ к вашей электронной почте, они не смогут получить доступ к вашему аккаунту.

Кодовое слово

В некоторых системах для подтверждения вашей личности и снятии блокировки ЛК может использоваться кодовое слово. Кодовое слово указывается при регистрации ЛК и нигде больше не отображается.

Интернет безопасность в социальных сетях

Интернет – отличный способ общаться со знакомыми со всех концов страны и даже мира. Здесь легко находить товарищей по интересам, можно слушать музыку, смотреть видео, играть. А еще онлайн можно встретиться с агрессивными троллями и провокаторами.

Агрессивные, оскорбительные или провокационные комментарии и посты, специально написанные для того, чтобы разозлить и расстроить оппонента. Пользователи, которые делают это, называются троллями. С помощью троллинга они самоутверждаются и привлекают к себе внимание.

Встретились с таким персонажем? Во-первых, не обижайтесь. Слова тролля не имеют к вам никакого отношения: он просто пытается поднять себе самооценку таким неприглядным способом. Во-вторых, не отвечайте. Тотальный игнор – лучший способ наказать тролля. Не пытайтесь доказать свою правоту, не приводите никаких аргументов – просто молчите.

Если неприятные комментарии вас расстраивают, забаньте (отправьте в черный список) их автора. В соцсетях это можно сделать самостоятельно, а если вас оскорбляют на форуме – обратитесь к модератору (пользователь форума или сайта, который следит за соблюдением правил ресурса. Он имеет право редактировать и удалять сообщения других пользователей вносить их в черный список (банить)).

Иногда в интернете можно встретить очень унизительные обобщения. Некоторые пользователи враждебно высказываются в адрес целой группы людей, у которых общая только национальность/религия/принадлежность к субкультуре. Вы наверняка видели обидные комментарии в адрес фанатов определенного стиля музыки. Ни в коем случае

нельзя разжигать ненависть к целой группе людей только потому, что они на вас не похожи. Это противозаконно. Поэтому никогда не участвуйте в такой травле, а если столкнетесь с таким в сети – сообщите администрации сервиса.

В социальных сетях можно встретить пользователей с фейковыми страницами (страницы с ложной информацией о владельце). Эти страницы могут собирать личную информацию о пользователях, быть прикрытием для мошенников, оставлять неприятные комментарии, предлагать участие в фейковых конкурсах, вымогать деньги. Признаки фейковой страницы в социальных сетях:

Аватарка отсутствует или на ней стоит изображение, загруженное из Интернета.

Личная информация отсутствует либо заполнена по минимуму.

Мало друзей и подписчиков.

Фотографии на странице загружены недавно.

Если страница действительно фейковая, после жалобы ее заблокируют.

Дети в интернете: правила поведения

Самое главное правило, которое вы должны донести до своего ребенка: если он столкнулся в сети с чем-то неприятным или непонятным, обязательно должен рассказать взрослым и попросить совета.

Обязательно объясните своим детям, почему очень важно тщательно отбирать фотографии и картинки для публикации в интернете. Ведь безобидная на первый взгляд шалость может повлечь за собой очень неприятные последствия, причем не только в сети, но и в реальной жизни.

Фотомонтаж с целью придания ему карикатурных черт называют фотожабой. Дети достаточно часто развлекаются подобным образом. В этом нет ничего страшного до тех пор, пока такая шутка не превращается в унижение. Даже дружеский шарж может обидеть того, над кем подшутили, особенно если фотожаба была загружена в сеть без его согласия.

Поговорите с ребенком и объясните, что унижать других, даже в шутку, недопустимо.

В сети довольно часто встречаются злоумышленники, которые с готовностью пользуются доверчивостью (особенно детской) в своих интересах. Объясните ребенку, что не стоит общаться онлайн с незнакомыми взрослыми людьми. Научите ребенка сразу же рассказывать вам об этом. Объясните, что это может серьезно навредить ему. Научите ребенка каждый раз, когда он загружает фото в сеть, задавать себе вопрос: «Что другие смогут узнать по моей фотографии?». Преступники часто выбирают жертв для ограбления или похищения именно в интернете. Поэтому объясните ребенку, что никогда нельзя

публиковать в сети координаты и фотографии дома или школы, особенно если на изображении можно прочесть адрес.

Компьютерные игры

Компьютерные игры уже давно сравнялись по популярности с телевидением, музыкой и фильмами, а где-то даже превзошли их. Вы можете помочь своим детям играть в занимательные и даже поучительные игры. И, само собой, соответствующие возрасту юного поколения. Нужно только придерживаться приведенных советов.

Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры.

Ребенок должен играть только с лично знакомыми; не вести переписку с незнакомыми и никогда не выдавать личную информацию, в том числе настоящее имя и место жительства. Контролируйте чаты и сообщения во время игр. Попросите детей сообщать вам, если игрок употребляет нецензурные слова; в этом случае можно выделить обидчика в списке и отключить или заблокировать его сообщения. Другой вариант сообщить о «нехорошем» человеке администраторам игры по электронной почте, в чате или другим способом.

Посоветуйте детям никогда не выдавать в чате личную информацию (например, имя, пол или домашний адрес), фотографии и не соглашаться на встречи. Убедитесь, что дети знают о необходимости сообщить вам в случае чего. Выбирайте соответствующие имена. Заставьте ребенка использовать имена героев, соответствующие игровым правилам. Эти имена не должны раскрывать никакую личную информацию или провоцировать домогательство. Скажите детям, что если кто-либо из игроков будет вести себя оскорбительно, игру следует остановить и немедленно сообщить вам. Безопаснее всего для детей играть через интернет вместе с вами. Возможно, им этого хочется меньше всего на свете (особенно тем, кто постарше), но это очень хороший способ научиться общению в Сети.

Множество детей обожают искать развлечения (например, игры) в интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако им нельзя играть в азартные игры на деньги. В чем разница между игровыми сайтами и сайтами с азартными играми? На игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди

выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Родительский контроль

Для контроля детей в сети Интернет существуют специальные программы родительского контроля, предназначенные, в первую очередь, для создания ограничений ребенку. Они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра сайтов. Все очень просто: на одни страницы заходить можно, на другие нельзя. Ограничения устанавливаются в автоматическом режиме через настройки программы.

Заслуженной популярностью пользуется программа родительского контроля Kaspersky Safe Kids. Помимо защиты ребенка от опасностей интернета она позволяет контролировать время использования ребенком устройства, сообщает данные о местонахождении ребенка и заряде батареи устройства, осуществляет мониторинг активности в Facebook и Вконтакте. Более подробно с возможностями программы можно ознакомиться на сайте разработчика https://www.kaspersky.ru/safe-kids, а также в специальном разделе на портале «Цифровой гражданин Югры» (http://eduhmao.ru/safekids/).

В завершение данного модуля, подведем итоги:

Никогда не переходите по ссылкам, присланным вам неизвестными людьми, эти ресурсы могут содержать вредоносный вирус, который украдет ваши данные от соц. сетей, и ваши личные данные станут доступны мошенникам. Собственно вредоносная ссылка может прийти и от вашего друга, ведь его могли взломать, например, в этом случае просто спросите друга, что это за ссылка, обычно их рассылает программа и ответа вы не получите. Перед тем как перейти по ссылке внимательно посмотрите, на какой ресурс она вас перенаправляет.

Если что-то нужно сохранить в тайне, лучше вообще не писать об этом в интернете – даже в постах с ограниченным доступом или в личных сообщениях. Ведь аккаунт могут взломать злоумышленники. Для взлома вашей странички, хакерам не всегда нужны дополнительные программы, иногда, бывает достаточным данных, которые вы сами о себе оставили в сети интернет. Ему лишь необходимо вбить, в поисковик ваше имя. Далее хакер просто нажмет кнопочку «забыли пароль» и по простому вопросу для восстановления, который вы придумали, например имя собаки получит доступ к вашему аккаунту. Поэтому, настоятельно рекомендуется брать вопрос на восстановление аккаунта не из списка, а придумывать его самому.

В настоящее время существует множество программ для скачивание контента с социальных сетей, первый на этом месте сеть Вконтакте, где, как известно содержится огромное количество пиратского контента. Приложения для скачивания обычно распространяются бесплатно, но подумайте, кто будет делать, что то просто так, правильно никто. Обычно они несут в себе кроме основных функций много рекламы, и поскольку в них надо вводить ваш пароль и логин, они могут быть опасны потому как вы передаете в чужие руки ваши данные.

Существуют аккаунты с многомиллионным количеством друзей или подписчиков, но обычно у владельцев таких аккаунтов информация или скрыта или не является действительной. Чтобы избежать проблем, не добавляйте неизвестных людей в друзья, поскольку информация, которую они могут узнать может применяться во вред вам.

Не доверяйте социальным сетям как самому себе, это всего лишь сайт, цель которого заработок денег и то, что они якобы гарантируют сохранность ваших данных, в действительности не гарантирует этого.

Модуль 4. Меры предосторожности при проведении Интернет-транзакций

Основные понятия, связанные с онлайн-платежами.

Электронные деньги работают так же, как и обычные наличные – ими можно оплатить товар или услугу. Разница в том, что они лежат на электронном носителе: банковской карте, счету электронной платежной системы или в электронном кошельке.

Банковская карта – пластиковая карта, которая привязана к одному или нескольким расчетным счетам в банке. Ей можно оплачивать товары и услуги, в том числе онлайн, и снимать наличные деньги в банкоматах и операционных кассах. По сути, это физический символ вашего банковского счета, который можно потрогать и предъявить.

С дебетовой карты можно потратить только то, что есть у вас на счету. А вот израсходованные с кредитной карты средства вы автоматически берете у банка в кредит и обязаны вернуть с процентами.

Мобильный и интернет-банкинг – услуга, которая позволяет клиенту банка совершать операции по собственным счетам с мобильного устройства или через браузер на специальном сайте. Необходимо иметь доступ в интернет и знать логин и пароль для входа в личный кабинет.

Электронный кошелек – это специальная программа или интернет-сервис, с помощью которых можно хранить электронные деньги и платить ими. По сути это аналог банковского счета. Самые известные: Яндекс.Деньги и кошелек платежной системы QIWI. Бывают и в виде физических носителей: карта московского метро «Тройка» и сим-карта

сотового оператора – это тоже электронные кошельки. Пополнять их можно через терминалы, с банковской карты или со счета мобильного телефона. Напрямую снять деньги с такого кошелька нельзя. Придется сначала перевести их на банковскую карту и дойти до банкомата.

Электронная платежная система – это система расчетов через интернет. Самые известные – WebMoney и PayPal. Чтобы использовать такую систему, и отправитель, и получатель денег должны быть в ней зарегистрированы. Переводить деньги можно с электронного кошелька или напрямую с банковской карты. При покупке с рублевой карты в зарубежном магазине происходит автоматическая конвертация в валюту продавца по собственному курсу платежной системы. Главная задача электронной платежной системы – гарантия безопасности операции для обеих сторон. PayPal, например, возвращает деньги, если покупку не доставили или товар не соответствует описанию.

Какую карту выбрать

Для оплаты вы можете использовать карту любой платежной системы: МИР, Visa или MasterCard. Обязательно обратите внимание на категорию карты, поскольку некоторые зарубежные торговые площадки не работают с самыми базовыми (Visa Electron, MasterCard Maestro и Electronic). А вот в каком банке вы ее откроете, особой роли не играет. Не забудьте узнать, как быстро пополнять карту и можно ли застраховать лежащие на ней средства.

Отдельная карта

Заядлым онлайн-покупателям советуем завести отдельную карту для шопинга в сети. Попросите свой банк выпустить дополнительную дебетовую карту, на которую будете переводить нужную сумму непосредственно перед покупкой. Так, если ее данные будут похищены, ваши основные сбережения не пострадают.

Лучше вообще не хранить крупные суммы денег на карте, которой пользуетесь ежедневно. Получили зарплату? Переведите ее на счет, к которому не привязано вообще никаких карт, а уже с него закидывайте мелкие суммы на основную.

Также стоит подумать о выпуске виртуальной карты. Оформить ее можно онлайн. Выдается специально для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с ее помощью нельзя.

Электронная платежная система или кошелек

Некоторые зарубежные продавцы принимают деньги только через электронные платежные системы (самые известные — WebMoney и PayPal). Это удобно: вы можете переводить деньги с привязанной к кошельку банковской карты, но продавец не увидит ее реквизиты. Электронная платежная система гарантирует безопасность сделки для обеих сторон.

Техника безопасности

Покупайте только на сайтах с отличной репутацией. Чем дольше существует магазин и чем больше о нем положительных отзывов, тем лучше.

Вводите конфиденциальные данные только на защищенных страницах. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета. Это значит, что данные передаются в зашифрованном виде и надежно защищены.

Подключите СМС-оповещения. Большинство банков поддерживают технологию верификации 3D-Secure. При совершении операции вам приходит сообщение с кодом подтверждения транзакции, который нужно ввести в специальном окошке на платежной странице. Поэтому важно сообщать в банк, если у вас украли телефон или вы сменили номер.

Если у вас украли деньги с карточки, сразу же позвоните в банк, чтобы сообщить об этом и заблокировать карту. По закону (№ 161-ФЗ, статья 9) обратиться с заявлением о несанкционированном списании нужно сразу же, как только это произошло, максимум на следующий день после получения уведомления о совершенной операции. Если опоздаете, банк не будет нести никакой ответственности за ваши пропавшие средства.

Единая биометрическая система

Данная система предоставляет новый уровень безопасности для пользователей портала госуслуг и проведения финансовых операций. Ваши биометрические данные привязываются к учетной записи на портале госуслуг. Биометрия помогает клиентам банков получать дистанционно услуги, для которых раньше нужно было приходить лично: например, открыть счет или получить кредит. В будущем это распространится на другие отрасли, в том числе – на государственные услуги.

Сдавать биометрию необязательно. Вы сами решаете, предоставлять биометрические данные или нет. В любой момент вы можете их удалить из учетной записи Госуслуг.

Как зарегистрировать биометрию

1. Найдите на карте ближайшее отделение банка и посетите его.

Чтобы зарегистрировать биометрию, вы должны быть клиентом банка и иметь подтвержденную учетную запись на Госуслугах. Если вы не клиент банка, сотрудник

поможет заключить договор и при необходимости подтвердит учетную запись на портале госуслуг. Возьмите с собой паспорт и СНИЛС.

2. Сотрудник банка сделает ваше фото и запишет голос.

Ваш биометрический шаблон попадет в Единую биометрическую систему. Это безопасно: данные передаются в обезличенном и зашифрованном виде. Через три года данные нужно будет обновить.

Как пользоваться услугами с биометрией?

Выберите услугу на сайте или в приложении банка. Чтобы получить ее дистанционно, авторизуйтесь с помощью учетной записи Госуслуг, а затем подтвердите личность при помощи биометрических данных: посмотрите в камеру и произнесите цифры, которые увидите на экране. Это можно сделать как на сайте банка, так и в мобильном приложении Единой биометрической системы, его можно скачать в Google Play и App Store.

Достаточно подтвердить операцию на сайте банка или в приложении «Биометрия» от Ростелеком. Для этого нужно выбрать услугу и подтвердить личность, посмотрев в камеру и произнеся цифры.

Единая биометрическая система разработана ПАО «Ростелеком» по инициативе Банка России и Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Федеральный закон 482-ФЗ регулирует передачу биометрических данных. Основная информация – в ст. 4 и 8

Покупаем в интернете: безопасно и просто

Не надо тратить время и силы на дорогу и общение с консультантами, можно внимательно изучить товар и сравнить стоимость у нескольких продавцов, есть время обдумать и решить, нужна ли вам эта покупка.

Недостатки у интернет-шопинга тоже есть. Во-первых, вас могут обмануть мошенники. Во-вторых, реальный товар может оказаться гораздо хуже, чем его виртуальный светлый образ.

Как могут обмануть?

Не доставить покупку

Некоторые интернет-магазины работают по полной предоплате. Иногда после этого вы можете получить некачественный товар или вовсе не увидеть свою покупку.

Привезти заведомо неисправный товар

Часто курьер торопится, поэтому вы не можете внимательно осмотреть приобретение. А когда позже обнаруживаете, что товар бракованный, вам отказываются его менять под предлогом, что вы сами испортили вещь.

Подписать на спам

Недобросовестные онлайн-продавцы требуют указать не только номер телефона для связи, но и другую личную информацию, которая к покупке никак не относится. А потом подпишут вас на спам и рекламные звонки.

Фишинговый сайт

Некоторые сайты лишь маскируются под интернет-магазин. На самом деле все, что им нужно — выманить данные вашей банковской карты вместе с секретным кодом, чтобы украсть ваши сбережения.

Нелегальные товары

Некоторые товары, которые продаются в иностранных интернет-магазинах, в России могут быть запрещены. Поэтому будьте внимательны, прежде чем покупать то, что у нас вообще не продается. Возможно, это не случайно.

На что обратить внимание?

На адресную строку браузера

Страницы ввода конфиденциальных данных любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета.

На отзывы покупателей.

Всегда читайте отзывы о магазине, в котором хотите сделать покупку. На Яндекс.Маркете можно посмотреть рейтинг торговой площадки. А крупные зарубежные интернет-магазины (например, Aliexpress) настолько дорожат своей репутацией, что у них даже есть собственные программы защиты покупателей, по которым можно вернуть деньги, если посылка, например, потеряется.

На наличие чека

Без чека вы точно не сможете обменять бракованный товар или вернуть деньги.

Что вы сообщаете о себе

Для курьера достаточно адреса, имени и номера телефона для связи. Некоторые службы доставки (например, BoxBerry) требуют обязательно вводить паспортные данные. Без этого вы не сможете завершить оформление заказа, да и получать посылку нужно только лично с паспортом.

На фотографии товара

Чаще всего магазины сами делают фотосессии, чтобы показать товар с наилучшей стороны. Украденные на других ресурсах изображения – повод насторожиться.

На слишком низкую цену

Не спешите радоваться, что нашли смартфон последней модели по цене в два раза ниже рынка. Скорее всего, товар проблемный: поддельный, с дефектами или даже краденый. А еще невероятно низкая цена – любимая уловка мошенников, и вас просто заманивают, чтобы потом обмануть.

Что еще можно сделать?

Внимательно читайте условия

Обязательно прочтите об условиях обмена и возврата товара, уточните, какие подтверждающие покупку документы вам выдадут. Проверьте, указаны ли контакты для связи. Чем больше информации о себе предоставляет торговая площадка, тем она надежнее.

Избегайте предоплаты

По возможности оплачивайте товар курьеру при получении и только после того, как проверите покупку. Если предоплата – обязательное условия торговой площадки, пользуйтесь проверенными платежными системами с программой защиты покупателей (например, PayPal) или заведите специальную виртуальную карту для онлайн-шопинга.

Тщательно проверяйте покупку перед оплатой

Даже если курьер утверждает, что очень спешит – распечатайте и проверьте свое приобретение в его присутствии. Это ваше законное право.

Проверьте интернет-страницу

На сайте Технический центр Интернет (http://www.tcinet.ru/whois/)можно узнать, когда был создан сайт и на кого он зарегистрирован. Домен, зарегистрированный давно и на собственное юрлицо торговой площадки – хороший знак. А вот злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

Изучите гарантийные условия и таможенные правила

Покупаете технику в зарубежном интернет-магазине? Обязательно изучите условия ее гарантийного обслуживания у нас в стране: есть ли официальные мастерские, какие документы вам потребуются, чтобы обратиться туда, можно ли при необходимости обменять товар в России.

Дорогостоящие товары могут облагаться таможенной пошлиной. Обязательно уточните этот вопрос покупкой. Иногда таможенный сбор сильно увеличивает цену приобретения.

Онлайн-аукционы и доски объявлений

Как правило, на таких площадках торгуют частные продавцы, продающие штучный товар. Но и полноценные интернет-магазины тоже часто имеют там представительства.

Шопинг на подобных сайтах может быть вполне безопасен, особенно с программой защиты покупателей.

Покупаете у частника? Будьте готовы к тому, что чек вам не выдадут, а обменять товар в случае брака, возможно, будет не на что.

Модуль 5. Защита персональных данных

Что такое персональные данные

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся, всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится. Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются. Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;

кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;

с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;

и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.

Получается, что персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, их совокупность, которые необходимы и достаточны для идентификации какого-то человека.

Как не допустить распространение персональных данных в интернете

Основные способы защиты персональных данных в интернете:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете, и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.
4. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
5. Старайтесь периодически менять пароли.
6. Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и так далее).

Как работает закон о «праве на забвение»

Какую информацию можно удалить

По закону о «праве на забвение» вы имеете право потребовать у поисковой системы удалить из результатов поиска ссылки на материалы, где речь идет о вас. При этом информация должна быть недостоверной, устаревшей (о событиях трехлетней давности или более ранних) или противоречить законам РФ. Важный нюанс: контент не смогут удалить с сайта, на котором он размещен, но информация пропадет из поисковой выдачи. Чтобы выйти на нее, понадобится знать точный адрес прямой ссылки.

По закону, контент, который вы просите удалить, должен иметь прямое отношение лично к вам: ФИО или внешность (если речь идет о фотографиях и видео) того, о ком идет речь в публикациях, должны совпадать с вашими.

Какую информацию удалить нельзя

Если информация недостоверна или противозаконна, вы можете требовать ее удаления без всяких оговорок. А вот для устаревших данных есть исключения.

Нельзя требовать удаления материалов, в которых есть признаки уголовных преступлений, если срок привлечения к ответственности по ним еще не вышел. То есть, если о вас написали, что вы украли деньги из бюджета, ссылки на статьи об этом можно будет удалить только после того, как (и если) вы докажете свою невиновность. Также нельзя требовать удаления материалов, где говорится о вашей судимости, если она не снята и не погашена.

Куда обращаться

Важно понимать, что в каждый поисковик нужно будет написать отдельное заявление. Его можно направить заказным письмом или заполнить специальную форму онлайн. Вот где это сделать:

Яндекс (+ Рамблер) https://yandex.ru/support/abuse/troubleshooting/oblivion.html

Гугл https://support.google.com/legal/contact/lr_legalother?product=websearch

Поиск@mail.ru https://go.mail.ru/support/oblivion/

Спутник http://corp.sputnik.ru/forgetform

Bing https://www.microsoft.com/ru-ru/concern/bing

Как подать заявление

Самостоятельно соберите все ссылки, которые хотите удалить из поисковой выдачи. Если через какое-то время обнаружатся новые материалы, придется подать еще одно заявление. Убедитесь, что информация по этим ссылкам относится непосредственно к вам. То есть, вас можно точно опознать по ФИО или по внешности, если речь о фотографиях и видео. Если указываете другие признаки (например, место работы и должность), дополнительно объясните, почему по ним легко узнать именно вас. Вам также придется доказать, что заявитель и жертва — одно и то же лицо (вы).

Подать заявление за другого человека нельзя, кроме случаев, если вы – родитель или официальный опекун пострадавшего. В таком случае нужно приложить сканы свидетельства о рождении ребенка и страницы из паспорта родителя с указанием родства.

Дальше следуйте инструкции:

Впишите свои персональные данные и актуальные контакты (достаточно будет адреса электронной почты), чтобы сотрудники поисковика могли связаться с вами.

Приложите скан паспорта.

Скопируйте все ссылки, которые хотите удалить из поисковой выдачи. Важно, чтобы это были прямые ссылки на нежелательный контент.

Укажите категорию, к которой относится информация: недостоверная, неактуальная или противоправная.

Объясните, почему вы считаете эти данные некорректными. Если есть доказательства вашей позиции, приложите их (это может быть ссылка на другую информацию, говорящую в вашу пользу, сканы решения суда и т.п.)

Дайте поисковику согласие на обработку персональных данных.

Заявление будет обработано за 10 рабочих дней, в течение которых поисковик может запросить дополнительную информацию. У вас есть 10 рабочих дней со дня получения запроса, чтобы ее предоставить. После чего в течение следующих 10 рабочих дней по вашему заявлению примут решение. Если оно будет положительным, ссылки удалят. Отрицательное решение представители поисковика обязаны аргументировать – отказать просто так нельзя. Не согласны? Отказ можно обжаловать через суд по месту юридического адреса поисковика, либо вашему по месту жительства. Если вы выиграете, поисковик будет обязан удовлетворить ваш запрос, иначе ему грозит внушительный штраф.

Что еще важно помнить

Закон о «праве на забвение» не позволяет удалить информацию, но помогает существенно затруднить ее поиск.

Закон относится к российским поисковым системам и иностранным поисковикам, ведущим коммерческую деятельность на территории России (например, рекламирующим товары российских производителей на русском языке).

Собственные поисковые системы сайтов (например, блогов и социальных сетей) не попадают под действие закона. Исключение: сайты, в которые встроен поиск Яндекса.

Требовать у поисковика удалить нежелательный контент по закону о «праве на забвение» может только физическое лицо. Юридическим лицам придется сразу обращаться в суд.

Если заявление хочет подать несовершеннолетний, ему нужно попросить об этом родителей или официального опекуна.

Поисковик не имеет права разглашать информацию о том, что вы обратились с просьбой удалить информацию о себе.

Модуль 6. Кибербезопасность

Вспомним основные, актуальные на сегодняшний день, интернет-угрозы и способы защиты от них.

Вредоносные программы

В основе практически любой компьютерной атаки лежит вредоносная программа. На компьютер пользователя такая программа может попасть одним из следующих способов:

– через USB-флешки и другие съёмные носители;

– через электронную почту и системы обмена мгновенными сообщениями;

– через заражённые веб-страницы.

Рекомендации

Используйте средства антивирусной защиты.

Регулярно обновляйте базы данных антивируса.

Регулярно обновляйте программное обеспечение.

Работайте под учётной записью с ограниченными правами.

Отключайте автозапуск подключённых устройств.

Используйте межсетевой экран (firewall).

Используйте спам-фильтры.

Регулярно создавайте резервные копии.

Социальная инженерия

Этот термин обозначает способ получить нужную злоумышленнику информацию или заставить пользователя совершить необходимые действия, не используя технические средства, а только применяя психологические методы воздействия на людей: при помощи убеждения, внушения и хитрости. Стоит отметить, что любой пользователь сети Интернет уязвим к методам социальной инженерии. Основные пути воздействия на пользователя – это телефон, электронная почта, социальные сети и мессенджеры. В результате действий злоумышленника пользователи добровольно выдают свои данные и совершают действия, зачастую не подозревая, что их обманули.

Схемы мошенничества бывают разные:

Сбор денег «на лечение ребенка», когда злоумышленники делают рассылки писем якобы от лица благотворительных организаций с просьбами о пожертвованиях.

«Ошибочный платеж». Вам приходит СМС о поступлении денег на счет телефона, а через некоторое время телефонный звонок о якобы ошибочном платеже с просьбой о возврате денег.

Телефонные звонки от «сотрудников банка», которые в начале разговора сообщают человеку о том, что его деньги на карте в опасности и после этого выманивают у собеседника, находящегося в стрессовой ситуации, информацию о банковской карте.

Телефонные звонки от «сотрудников полиции», которые сообщают человеку о том, что его родственник задержан за преступление или является виновником ДТП и надо дать денег для решения «проблем».

Телефонные звонки от «организаторов лотерей», которые сообщают человеку о выигрыше в лотерею и надо оплатить какой-нибудь сбор для его получения. Обычно это не очень крупная сумма, поэтому не сразу возникает подозрение в обмане, тем более собеседник, как правило, отличный психолог и оратор.

Рекомендации

При благотворительности старайтесь сотрудничать только с хорошо известными благотворительными фондами. Посмотрите, как давно работает фонд, насколько полная контактная информация, свяжитесь с организаторами, почитайте отзывы.

При требовании вернуть ошибочный платеж проверьте номер отправителя СМС о поступлении платежа – мобильные операторы рассылают подобные уведомления с коротких, нестандартных номеров (например, у Tele2 это 8-353-2). На всякий случай проверьте баланс на счете телефона.

Никогда и никому не сообщайте информацию о банковских картах (срок действия, 3-х значный код с оборотной стороны карты), а также одноразовые коды доступа к карточному счету.

Обязательно свяжитесь с родственником, якобы попавшим в неприятную ситуацию.

Если письмо с просьбой о переводе денег пришло от знакомого Вам человека, перезвоните ему и спросите, действительно ли он это отправлял.

Не отвечайте на письма от неизвестных отправителей. Проверяйте личность отправителя (организации) письма через поисковые системы или официальные сайты.

Не переходите по ссылкам, содержащимся в письмах от неизвестных отправителей.

Не сообщайте приватную информацию, запрашиваемую в телефонных разговорах, письмах, приходящих по электронной почте и сообщениях в электронных мессенджерах.

Фишинг

Цель фишинга – получение злоумышленником данных банковской карты пользователя или информации об учётной записи (логине и пароле) на каком-либо ресурсе в сети Интернет. Инструмент фишинга – поддельная страница сайта с формой для ввода данных или письмо, отправленное якобы от лица администрации или службы поддержки

этого онлайн-ресурса, содержащее ссылку на поддельную страницу. Дизайн формы для ввода данных или поддельного сайта может быть довольно точной копией настоящего ресурса.

Рекомендации

Не переходите по ссылкам и не открывайте вложения из писем от неизвестных Вам адресатов.

Не сообщайте никому свои логины и пароли учётных записей, а также данные банковских карт.

Обращайте внимание на URL-адреса страниц, на которых Вы вводите учётные данные.

Проверяйте наличие https-соединения для сайтов, на которых Вы собираетесь ввести учётные данные.

Проверяйте реальные адреса гиперссылок, наводя на них курсор. Адрес, куда ведёт эта ссылка, будет отображён в левой нижней части браузера.

Поддельные антивирусы

Поддельные антивирусы могут быть как бесполезной утилитой, приобретенной пользователем за деньги, так и вредоносным программным обеспечением, похищающим данные с компьютера. Фальшивый антивирус можно получить различными способами. Например, скачав с сомнительного сайта бесплатный антивирус, гарантирующий стопроцентную защиту от всех видов вредоносных программ. Кроме того, поддельные антивирусы распространяются как вложения электронной почты, могут загружаться на уже зараженный компьютер специальным вирусом-загрузчиком.

Рекомендации

Используйте только лицензионные антивирусные средства.

Скачивайте антивирус только с официального сайта разработчика.

Регулярно обновляйте антивирус (обновления должны также загружаться из официальных источников).

Фальшивая техподдержка

Фальшивая техподдержка является одним из методов социальной инженерии. Обычно это звонки по телефону якобы от сотрудников банка или технических специалистов какой-нибудь крупной компании, занимающейся разработкой программного обеспечения. Злоумышленники заявляют об обнаружении вирусов на компьютере жертвы и, используя непонятные большинству пользователей технические термины, пытаются убедить собеседника предоставить им удалённый доступ к компьютеру или сообщить пароли от учётных записей.

Рекомендации

Если Вы получили письмо на электронную почту якобы от сотрудника компании Microsoft или Apple, не сообщайте ему логины и пароли от Ваших учётных записей и не предоставляйте ему удалённый доступ к Вашему компьютеру.

Помните, что сотрудники банка не имеют права требовать сообщить им пин-код или CVV/CVC-код Вашей карты.

Контрафактное программное обеспечение

Скачивая пиратское программное обеспечение, пользователь рискует безопасностью компьютера и своих данных, а также подвергает опасности взлома устройства других пользователей. Использование контрафактного программного обеспечения может привести к нежелательным последствиям.

Рекомендации

Используйте лицензионное программное обеспечение.

Используйте программное обеспечение с открытым исходным кодом (open source).

Избегайте передачи личных данных с компьютера, на котором установлено контрафактное программное обеспечение. Регулярно обновляйте антивирусные базы данных и операционную систему.

Список источников и литературы

1. Гюлджян А. Г. Информатизация общества как одна из важнейших составляющих социального прогресса // Молодой ученый. — 2017. — №32. — С. 12-15. — URL https://moluch.ru/archive/166/45367/ (дата обращения: 03.04.2019).
2. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. - 324 с.
3. Региональный общественный центр интернет-технологий https://rocit.ru
4. Anti-malware.ru – информационная безопасность для профессионалов https://www.anti-malware.ru/
5. Персональныеданные.дети http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/
6. © Public-pc.com Источник: https://public-pc.com/web-swindler/
7. https://www.compgramotnost.ru/zdorove-kompyutera/fishingovyj-sajt-eto