Лекция 20

ҚАЗАҚСТАННЫҢ АШЫҚ УНИВЕРСИТЕТІ

# ПСИХОЛОГИЯ ИНТЕРНЕТА

## Защита данных в интернете

Проведение финансовых операций с использованием интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам, передача телефонных разговоров требуют обеспечения соответствующего уровня безопасности.

Конфиденциальная информация, которая передается по сети интернет, проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет пункта назначения.

Проблемы безопасности передачи можно разделить на четыре основных типа:

- Перехват информации – целостность информации сохраняется, но ее конфиденциальность нарушена.
- Модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату.
- Подмена авторства информации.
- Перехват сообщения с его изъятием.

Обычно маршрутизаторы не отслеживают проходящие сквозь них потоки информации, но возможность того, что информация может быть перехвачена, существует. Более того, информация может быть изменена и передана адресату в измененном виде. К сожалению, сама архитектура сети интернет всегда оставляет возможность для недобросовестного пользователя осуществить подобные действия.

Характеристики безопасности системы:

1. Аутентификация – это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий.
2. Целостность – состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий.
3. Секретность – предотвращение несанкционированного доступа к информации.

Для обеспечения секретности применяется **шифрование, или криптография**, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа. В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм – это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Оно может быть интерпретировано только с помощью ключа. Очевидно, чтобы зашифровать послание, достаточно алгоритма.

Следующий способ защиты – **электронно-цифровая подпись** (ЭЦП). Это реквизит электронного документа, предназначенный для отличия его от подделки. ЭЦП создается в результате криптографического преобразования информации с использованием закрытого ключа и позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронно-цифровая подпись – это программно-криптографическое средство, которое обеспечивает:

- Проверку целостности документов.
- Конфиденциальность документов.
- Установление лица, отправившего документ.

Использование электронно-цифровой подписи позволяет:

- Значительно сократить время, затрачиваемое на оформление сделки и обмен документацией.
- Усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов.
- Гарантировать достоверность документации.
- Минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена.
- Построить корпоративную систему обмена документами.

Существует три вида электронно-цифровой подписи: простая, усиленная неквалифицированная и усиленная квалифицированная электронно-цифровая подпись.

С помощью использования кодов, паролей или иных средств простая электронно-цифровая подпись подтверждает факт формирования электронной подписи определенным лицом. Простая электронно-цифровая подпись имеет низкую степень защиты. Она позволяет лишь определить автора документа и не защищает документ от подделки.

Усиленная неквалифицированная электронно-цифровая подпись:

1) Получена в результате криптографического преобразования информации с использованием ключа электронной подписи.
2) Позволяет определить лицо, подписавшее электронный документ.
3) Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.
4) Создается с использованием средств электронной подписи.

Усиленная неквалифицированная электронно-цифровая подпись имеет среднюю степень защиты. И чтобы ее использовать, необходим сертификат ключа ее проверки.

**Аутентификация** является одним из самых важных компонентов. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдает.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передает управление серверу аутентификации.

Для защиты корпоративных информационных сетей используются брандмауэры – система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.

**Фишинг** – это один из видов мошенничества, направленный на хищение ценных личных данных пользователя, таких как номера кредитных карт, пароли, сведения о банковских счетах и др. Становясь все изобретательнее, мошенники постоянно совершенствуют фишинг-сообщения электронной почты и всплывающие окна. Они часто используют официальные эмблемы реальных организаций и другие идентифицирующие сведения, полученные непосредственно с подлинных веб-узлов. Чтобы придать фишинг-сообщению большую убедительность, мошенники могут поместить в него ссылку, которая якобы указывает на подлинный веб-узел, но на самом деле приводит на мошеннический сайт, выглядит так же, как официальный веб-узел.

Как распознать мошенническое сообщение электронной почты? Некоторые примеры фраз, часто используемых в сообщениях электронной почты при проведении фишинг-атак:

1. «Подтвердите свою учетную запись». Представители компаний не должны запрашивать по электронной почте пароли, имена пользователей, номера социального страхования и другие личные сведения.

Получив сообщение электронной почты от корпорации Microsoft с просьбой обновить информацию о кредитной карте, не отвечайте — это мошенническое сообщение.

2. «Если вы не ответите в течение ближайших 48 часов, ваша учетная запись будет заблокирована». Такие сообщения вызывают ощущение срочности, чтобы заставить человека ответить, не раздумывая.

3. «Уважаемый клиент»! Фишинг-сообщения обычно рассылаются массово и не содержат ни имени, ни фамилии получателя.

4. «Кликните ссылку ниже, чтобы получить доступ к своей учетной записи». Ссылки, по которым просят перейти, могут полностью или частично содержать реальное имя компании и обычно замаскированы. Они ведут на другой адрес, как правило, на мошеннический веб-узел.

Мошенники также используют URL-адреса, которые напоминают названия известных компаний, но при этом слегка отличаются от них: некоторые буквы могут быть добавлены, пропущены или переставлены.

## Программы-шпионы и вирусы

Интернет-злоумышленники могут использовать вирус, чтобы одновременно установить контроль над большим количеством компьютеров и использовать их в качестве зомби, которые образуют мощную сеть, осуществляющую вредоносную деятельность.

**Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Основная цель вируса – его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов. Это удаление файлов и даже операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

Сети зомби, в которые могут входить до 100 000 компьютеров, используются для рассылки нежелательной почты, распространения вирусов, атак на другие компьютеры и серверы, а также совершения иных видов преступлений и мошенничества. Вирус, который превращает компьютер в зомби, может вызвать отображение странных сообщений, замедление работы компьютера или его неожиданное поведение. Такие вирусы обычно не отключают компьютер, так как для работы сетей зомби необходимо, чтобы входящие в них компьютеры были подключены к интернету.

Сутью данного способа является самый обыкновенный шантаж с вымогательством денег, только делается все это с помощью интернета.

**1. Вирус с сюрпризом.**
Попадая на компьютер пользователя, этот вирус блокирует работу операционной системы, помещая на рабочем столе сообщение о том, что для восстановления работы машины необходимо куда-то перечислить определенную сумму денег.

**2. «Украденные» средства коммуникации.** Взломы чужих аккаунтов, электронных ящиков, «мессенджеров». Настоящему владельцу предлагается выкупить свои же пароли у хакера, которые тот взломал и сменил.

**3. Разглашение личной информации.** Украденные с чужого компьютера материалы часто могут оказаться более ценными, нежели данные о паролях и денежные счета.

Приведем пример. Пользователь А непрерывно терроризирует пользователя Б с помощью интернета и других электронных средств связи. Орудиями киберпреследователя являются электронная почта, мессенджеры, форумы, чаты, социальные сети. Кроме того, сеть позволяет злоумышленнику остаться анонимным. Вычислить преследователя без применения специальных средств очень сложно, а в ряде случаев почти невозможно.

Как избежать киберпреследования? Главное – оставлять как можно меньше информации о себе в сети, этим вы усложняете злоумышленнику работу по добыче ваших контактов. Нужно быть осмотрительными в процессе общения.

По материалам сайта телеканала КТК, директор компании «Informsecurity», эксперт в области корпоративной и информационной безопасности Игорь Чернов предлагает семь способов защиты, которые позволят обеспечить безопасность хранения данных:

**1. Надежные пароли.** Для защиты информации на рабочем компьютере в первую очередь нужно создать пароль к учетной записи. При необходимости вы можете легко заблокировать ваш компьютер: пуск – завершение работы – блокировать. При включении устройства надо будет также ввести пароль. На ноутбуке можно настроить блокировку при закрытии крышки. Для пущей безопасности можно установить пароль и на BIOS или жесткий диск. Пароль при этом должен быть надежный, иначе смысл его установки теряется. Воспользуйтесь специальным генератором и потрудитесь создать разные пароли для всех своих логинов. Это касается и аккаунтов в социальных сетях, и электронных почтовых ящиков. Запаролить можно

и важные документы. Главное не хранить ключи в файлах TXT, DOC, RTF. Лучше воспользоваться специальной программой для хранения паролей. Тогда вам останется запомнить только один пароль, а остальные вы найдете в списке.

**2. Актуальный антивирус.** Пожалуй, главная угроза персональной информации – это вирусы. Трояны, черви, клавиатурные шпионы и прочие вредоносные программы способны удалить, украсть или изменить ее. Чтобы защитить личные данные, желательно иметь актуальную версию антивирусного ПО с функциями брэндмауэра и файервола, а также быть аккуратным в сети – не скачивать непроверенные файлы с файлообменников, не переходить по подозрительным ссылкам и так далее.

**3. Двухфакторная аутентификация.** Эта система пока не очень распространена среди пользователей, но отличается своей эффективностью. Она предполагает не только надежный пароль, но и определенную информацию или факт, который известен исключительно пользователю. К примеру, это может быть его голос, отпечаток пальца, смарт-карта или что-то еще. Лишь бы доступ к этим факторам не имели посторонние лица.

**4. Использование протокола HTTPS.** Оплачивая что-либо в сети, нужно убедиться, поддерживает ли сервер протокол безопасной передачи данных HTTPS. В этом случае при проведении финансовых транзакций система присваивает клиенту уникальный сертификат, после чего все пересылаемые им данные кодируются 40, 56, 128 или 256-битным ключом. Дешифровка идет лишь на конечных устройствах, поэтому перехват такого сигнала злоумышленнику ничего не даст. Сайты интернет-магазинов, банков, а также платежных систем (Яндекс.Деньги, Webmoney) используют протокол HTTPS по умолчанию. Сервисы Facebook, Google, Twitter, Вконтакте предоставляют возможность его включения в настройках аккаунта. К ресурсам, не использующим данный протокол, стоит относиться очень осторожно.

**5. Защита беспроводных сетей.** Получить доступ к содержимому компьютера злоумышленники могут и через незащищенную сеть WiFi. Чтобы избежать этого, рекомендуется установить на маршрутизаторе метод шифрования данных WPA/WPA2 и придумать сложный пароль. Также обезопасить себя от взлома сети WiFi можно, отключив транслирование имени подключения (SSID). В этом случае подключиться к маршрутизатору смогут лишь те, кто знает точное имя сети.

**6. Шифрование данных.** Ценные данные на компьютере можно защитить с помощью шифрования. Такие программы, как Free Hide Folder, Folder Lock, TrueCrypt и другие, позволяют сделать это совершенно бесплатно. Кроме того, важные файлы можно запаковать в архив ZIP или RAR и поставить на них надежный пароль. Такой архив злоумышленник не сможет открыть, даже если получит полный доступ к вашему компьютеру.

**7. Системы родительского контроля.** Риск подхватить вирусы или стать объектом хакерской атаки значительно возрастает, если за компьютером сидят дети. Обезопасить себя в этом случае можно с помощью системы родительского контроля: она позволяет регламентировать время пребывания ребенка за компьютером, запрещает доступ к отдельным программам и сайтам, блокирует возможность установки ПО. Кроме того, для ребенка можно сделать отдельную учетную запись с ограниченными правами.

К сожалению, универсального способа защиты данных, который бы отличался стопроцентной эффективностью, не существует. Эксперты советуют комбинировать те или иные методы и периодически делать резервное копирование самой важной информации, чтобы максимально обезопасить себя от хакеров.