Методы, средства и технологии защиты информации в сети Интернет

Что такое данные, где они хранятся, как используются и зачем их защищать? Кому они вообще нужны и как их защищать?

Данные можно условно разделить на два вида:

- Персональная информация физического лица (фамилия, имя, отчество, данные паспортов (российского и заграничного), СНИЛС, ИНН, номера прав, данные своего автомобиля, номер телефона, адрес проживания, ФИО ближайших родственников и их данные и т.д.);
- Сведения компаний (юридического лица: как коммерческие, так и государственные организации). Сюда входят сведения о руководителе, о сотрудниках, конфиденциальные данные, представляющие коммерческую тайну (оборот компании, банковские счета, перечень контрагентов – поставщиков и покупателей) и так далее.

Информация хранится на бумаге – паспорт, СНИЛС, бумажные копии документов – и в электронном виде в сети Интернет, в программах кадровых служб, в базе данных операторов связи, у контрагентов и поставщиков услуг, товаров и т.д.

Пользователями информации являются представители государственной власти (МВД, ФСБ, судебные приставы), службы HR компаний, сотрудники коммерческих организаций. Цели самые разные: обзвон для предложения своих товаров и услуг, ознакомление с потенциальным работником перед наймом, контактные данные… И среди прочих, ищут персональные и корпоративные данные мошенники.

Одной из основных задач по обработке, хранению данных является предотвращение несанкционированного доступа к конфиденциальной информации. Задача эта решается путем выбора соответствующего метода защиты информации в сети. В теории все методы защиты информации в сети Интернет можно разбить на несколько больших групп:

- создание на пути угрозы (атаки) **препятствия** – в том числе ограничение физического доступа к носителям информации;
- **управление** уязвимостями и элементами защищаемой системы;
- осуществление комплекса мероприятий, результатом которых становится **маскировка** защищаемой информации (сюда можно отнести средства криптографического шифрования);
- разработка плана мероприятий, распределение ролей и уровней доступа (**регламентация**), при которых пользователи информационной системы (ИС) обязаны придерживаться заданных протоколов использования информации, снижающих риски несанкционированного доступа к сведениям.

Соблюдение правил доступа, обработки и хранения информации может достигаться за счет мер **принуждения** (в том числе угрозы административной, материальной, уголовной ответственности за нарушения) и **побуждения** (соблюдения установленных правил по морально-этическим и психологическим причинам).

Метод маскировки считается единственным надёжным способом защиты информации при ее передаче по каналами связи (в Интернете). В корпоративных и локальных сетях также высокую эффективность показывают следующие методы:

- идентификация пользователей, ресурсов компьютерной сети (через присвоение идентификаторов и аутентификации при каждом сеансе работы с данными из ИС, аутентификация может производиться посредством использования электронной цифровой подписи, ЭЦП, пары логин-пароль и иными средствами);
- регламентация доступов к любым ресурсам – контроль доступа и полномочий, ведение журнала учета обращений (запросов) к ИС, анализ соответствия запросов времени суток (с установлением границ рабочего времени), определение мер ограничения при несанкционированном доступе.

Средства защиты информации в сети Интернет

Средства защиты информации в Интернете бывают:

- техническими и технологическими:
  - физическими – устройствами и системами, создающими препятствия на пути злоумышленников или дестабилизирующих факторов, сюда относятся в том числе и двери, замки и т.д.;
  - аппаратными – устройствами, встраиваемыми в ИС специально для защиты информации (могут создавать препятствия или шифровать данные);
  - программными – специализированным программным обеспечением (ПО), реализующим функции создания препятствий действиям злоумышленников, шифрующими данные или распределяющим уровни доступа;
- законодательными – правовыми инструментами, стандартами (на уровне предприятия это могут быть нормативы, права доступа и т.д., включая устанавливающие материальную ответственность за небрежное или намеренное нарушение правил использования ИС);
- организационными, в том числе сложившаяся практика обработки информации.

К организационным методам защиты информации от ее последующего распространения в сети можно назвать:

- ограничение публикуемого контента в социальных сетях (путешествия, обстановку своего жилья, ФИО друзей, даты дней рождения, номера телефонов и другую контактную информацию);

- использование сотрудниками специально созданных и не связанных с корпоративными аккаунтами личных аккаунтов на avito.ru, youla.ru и прочих досках объявлений;
- контроль предоставления персональной информации в банках, налоговых органах, на вокзалах, в авиа/железнодорожных кассах, где могут быть посторонние «уши»;
- контроль публикуемой на бейджах линейного персонала информации о работниках – достаточно должности и имени (зная ФИО сотрудника несложно найти его профиль в социальных сетях, т.е. однозначно идентифицировать личность);
- уничтожение бумажных носителей информации (бланков, отчетов), содержащих конфиденциальные данные;
- ограничение использования корпоративных аккаунтов, email для прохождения регистрации и авторизации в социальных сетях, на сайтах, в мобильных приложениях;
- предоставление взвешенной информации о сотрудниках, организации на сайте, в социальных сетях (официальных страницах, группах).

Технологии защиты информации в сетях

Основным способом защиты передаваемых данных является их шифрование. Стойкость шифра зависит от сложности используемого алгоритма. Криптографические (математические) методы шифрования защищены от любых типов угроз, кроме физического доступа к носителям информации (с ключом шифрования).

Если передаваемые данные не являются секретными, а требуется лишь подтверждение их подлинности (подлинности подписей), то используется электронная цифровая подпись (ЭЦП). Подписанный ЭЦП электронный документ не защищен от несанкционированного доступа, однако не может быть изменен без сигнализации об этом.

Сетевые средства защиты информации

В общем случае, проникнуть в сеть предприятия можно только имея логин и пароль одного из пользователей, т.е. пройдя процедуру аутентификации. При передаче информации посредством сети Интернет возможен перехват пользовательских имени и пароля. Технически вопрос можно решить проведением дополнительной аутентификации машин-клиентов, двухфакторной системой авторизации, применением шифрования. Организационно – проведением аудита событий.

Защита беспроводной сети

С развитием беспроводных технологий и их доступностью в каждом доме и офисе появился wi-fi роутер. Но любое удобство несет за собой определенные риски. Сегодня на рынке стали доступны сканеры (снифферы – анализаторы) wi-fi сетей, которые могут получить данные паролей, установленных на Вашем беспроводном устройстве. Как защититься от взломщика?

1. Используйте защищенный пароль. Требования к паролям изложены ниже.
2. Регулярно обновляйте программное обеспечение роутера. Пригласите специалиста для этих целей. Данную процедуру проводите не реже чем раз в год.
3. Обязательно запишите пароль к вашему устройству, который вам установил мастер-наладчик оборудования.
4. Обязательно должен быть установлен формат шифрования сети WPA В ближайшее время появится стандарт шифрования WPA 3.

Программные средства защиты информации в сети

Одним из способов получения мошенниками логина и пароля для доступа в корпоративную сеть является метод подбора. Для начала злоумышленнику может потребоваться получить варианты логина, и сделать это можно путем сбора почтовых аккаунтов – с сайтов, социальных сетей и других профилей лиц, принимающих решения (ЛПР). Иногда ЛПР используют несколько почтовых аккаунтов, не только корпоративные. Получив тем доступ к личной почте, можно попробовать получить доступ уже к корпоративной (например, запросив пароль для ее восстановления). Как этому противостоять?

Большинство крупнейших почтовых сервисов и социальных сетей предлагают двухфакторную авторизацию – суть которой заключается в первичном вводе пароля, на втором шаге система авторизации сервиса просит ввести либо одноразовый код, либо код из специальных программ типа Google Authenticator* или Microsoft Authenticator.

Программы Authenticator обычно устанавливается на мобильный телефон и требует соединение с сетью Интернет. В режиме реального времени программа Authenticator генерирует одноразовые коды, которые требуются ввести на втором этапе авторизации пользователя.

Организационные методы защиты данных

Если Вы использовали Ваши аккаунты на корпоративных устройствах, либо в интернет-кафе – не поленитесь – нажмите кнопку «Выход» и очистите Ваши данные в браузере. Не ставьте галочку «Запомнить» ваши данные аккаунтов в браузере.
Также требуется защита персональных данных в крупнейших сервисах по продаже личных вещей типа avito.ru, youla.ru — данные сервисы научились ранжировать продаваемые товары по разным критериям, в число которых входит стоимость. Для защиты номера телефона при размещении объявлений в категории автомобили, сервисы предлагают замену фактически указанного номера на виртуальный и все звонки проходят через переадресацию. Вы как пользователь можете сами определять кому давать свой настоящий номер, а кому нет.

Защита данных на личном компьютере (ноутбуке)

Для хищения личных данных пользователей и компаний каждый день в сети появляются сотни вирусов, троянов, шпионских программ, программ-вымогателей, которые попадая на компьютер или ноутбук практически с первых секунд начинают либо кидать информацию в Интернет, либо ее шифровать. Как защититься? Правила простые:

1. Всегда используйте лицензионное программное обеспечение – операционную систему, офисные и антивирусные программы. Лицензионный софт постоянно обновляется – шанс подхватить вредоносное ПО значительно меньше. Заведите привычку раз в неделю проверять свое устройство антивирусом.
2. Не работайте на своем домашнем устройстве под пользователем администратором, заведите две учетные записи и работайте всегда под пользователем с ограниченными правами. Если лень это делать – приобретите устройство компании Apple, которое защищено лучше и включает в себя вышеизложенные пункты защиты.
3. Обязательно делайте резервные копии важной информации. В сети доступны за небольшие деньги облачные сервисы, которые позволяют надежно хранить ваши данные.

- mail.ru.
- yandex.ru.
- ru.

1. При серфинге в интернет и вводе данных обязательно обращайте внимание, что вы действительно находитесь на сайте нужно организации, а не на его клоне – фишинговый сайт.
2. Если к Вашему ноутбуку или компьютеру имеют доступ другие люди, не пользуйтесь сервисами хранения паролей на сайте.

Очень избитая тема – тема защиты паролей. В Интернете есть база скомпрометированных паролей — https://www.opennet.ru/opennews/art.shtml?num=48121, в которой содержится более 500 млн паролей. Проверьте пароли свои и своих сотрудников, не исключено, что и они так же окажутся в этой базе. Что делать? Придумайте свои интересные требования к паролям. К примеру, книга «Граф Монте-Кристо» заканчивается фразой «Ждать и надеяться!» в итоге получаем замечательный пароль на английском языке – «:lfnmbyfltznmcz!». Обязательно используйте и цифры, и символы, и буквы. Длину пароля задавайте не меньше 8 знаков. Думайте нестандартно. Обязательно раз квартал или полгода меняйте свои пароли к сервисам. Не используйте один и тот же пароль для всех сервисов.
Если же Вы не надеетесь на свою память – установите приложение для хранения паролей на свой мобильный телефон — https://lifehacker.ru/10-menedzherov-parolej/.
Часто в интернете требуется для авторизации на сервисе ввести личную почту или данные аккаунта от социальных сетей. Заведите себе дополнительный в аккаунт, который вы будете использовать для таких целей. Помните, что любая регистрация на сайтах в Интернете несет за собой СПАМ, и, если вы активный пользователь Интернета – дополнительный аккаунт – ваша защита. Внедрите такой же подход для своих сотрудников, используя метод **побуждения**.
* — компания-владелец нарушает законодательство РФ.