ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- *Информационная безопасность организации* – состояние защищенности информационной среды организации, обеспечивающее ее формирование, использование и развитие.

- *Информационная безопасность* (англ. information security) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.

Критерии информационной безопасности

Стандартная модель безопасности состоит из трех категорий:

1) конфиденциальность – доступность информации только определенному кругу лиц;

2) целостность – гарантия существования информации в исходном виде;

3) доступность – возможность получения информации авторизованным пользователем в нужное для него время.

Другие категории модели безопасности

- *аутентичность* или подлинность (англ. authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным, возможность установления автора информации;
- *неотказуемость* или апеллируемость (англ. non-repudiation) – возможность доказать, что автором является именно заявленный человек и никто другой.
- *подотчетность* (англ. accountability) – обеспечение идентификации субъекта доступа и регистрации его действий;
- *достоверность* (англ. reliability) – свойство соответствия предусмотренному поведению или результату.

Стандарты в области информационной безопасности:

- BS 7799-1:2005 Британский стандарт BS 7799 первая часть. Практические правила управления информационной безопасностью описывают 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* организации, определенных на основе лучших примеров мирового опыта (best practices) в данной области.

- ISO/EC 27001: 2005 «Информационные технологии - Технологии безопасности - Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

- ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации».

ГОСТ Р 51188-98 «Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство».

ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

ГОСТ Р ИСО/МЭК 15408-2-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».

ГОСТ Р ИСО/МЭК 15408 «Общие критерии оценки безопасности информационных технологий» – стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности, благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» – защита информации от несанкционированного доступа, модификации или утечки и другие способы защиты, реализуемые аппаратными и программными средствами.

ГОСТ Р ИСО/МЭК 1779 «Информационные технологии. Методы безопасности. Руководство по управлению безопасностью информации». Прямое применение международного стандарта с дополнением – ISO/IEC 17799:2005.

ГОСТ Р ИСО/МЭК 27001 «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта ISO/IEC 27001:2005.

ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты».

German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Действия, осуществляемые авторизованными пользователями:

1) целенаправленная кража или уничтожение данных на рабочей станции или сервере;

2) повреждение данных пользователем в результате неосторожных действий.

2. «Электронные» методы воздействия, осуществляемые хакерами:

1) несанкционированное проникновение в компьютерные сети.
2) DoS-атаки.
3) Компьютерные вирусы.
4) Спам.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

Атака типа DoS (сокр. от Denial of Service – «отказ в обслуживании») – это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Цель атакующих – сделать недоступным из Интернета тот или иной ресурс. Чаще всего это просто блокирование доступа, иногда вывод этого ресурса из строя.

Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т.п.

Компьютерные вирусы

- небольшая ПО объему компьютерная программа, обладающая следующими свойствами:

- возможностью создавать свои копии и внедрять их в другие программы;
- скрытность (латентность) существования до определенною момента;
- несанкционированность (со стороны пользователя) производимых ею действий;
- наличие отрицательных последствий от ее функционирования.

Не все программы, обычно называемые вирусами, обладают всеми из перечисленных свойств.

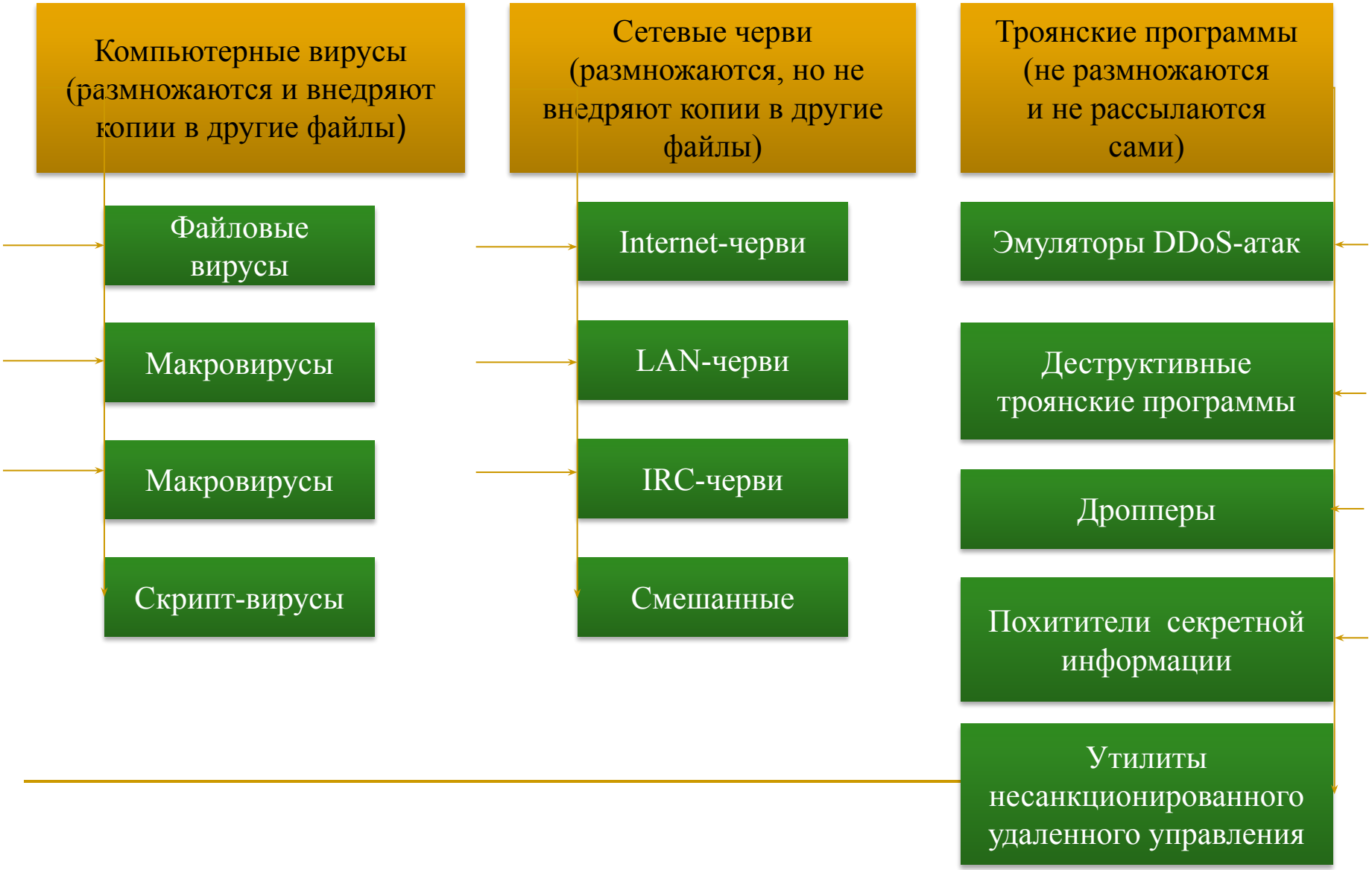
Компьютерным вирусам, как и биологическим, характерны определенные *стадии существования*:

1) *латентная* стадия, в которой вирусом никаких действий не предпринимается;
2) *инкубационная* стадия, в которой основная задача вируса - создать как можно больше своих копий и внедрить их в среду обитания;
3) *активная* стадия, в которой вирус, продолжая размножаться, проявляется и выполняет свои деструктивные действия.

По среде обитания вирусы можно разделить на

- файловые;
- загрузочные;
- файлово-загрузочные;
- сетевые;
- макровирусы.

Классификация вредоносных программ



3. «Естественные» угрозы:

Возможные варианты утечки конфиденциальной информации, хранящейся на жестких дисках и лентах:

- размещение серверов в стороннем центре данных (collocation);
- отправка серверов или жестких дисков в ремонт;
- перевозка компьютеров из одного офиса в другой, например, при переезде;
- утилизация компьютеров, серверов, жестких дисков и лент;
- хранение магнитных лент в специальном депозитарии (off-site storage);
- перевозка ленты, например, в депозитарий;
- кража или потеря жестких дисков или лент.
- неправильное хранение,
- кража компьютеров и носителей,
- форс-мажорные обстоятельства и т.д.

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Система защиты - это совокупность специальных мер правового и административного характера, организационных мероприятий, программно-аппаратных средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

- По убеждению экспертов «Лаборатории Касперского», задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т.д.) должны применяться одновременно и под централизованным управлением.

Для построения эффективной системы защиты необходимо провести следующие работы:

- определить угрозы безопасности информации;
- выявить возможные каналы утечки информации и несанкционированного доступа (НСД) к данным;
- построить модель потенциального нарушителя;
- выбрать соответствующие меры, методы, механизмы и средства защиты.

Проблема создания системы защиты информации включает две задачи:

- разработка системы защиты информации;
- оценка разработанной системы защиты информации.

В настоящее время существует большое количество *методов обеспечения информационной безопасности:*

- средства идентификации и аутентификации пользователей (так называемый «комплекс 3А»);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;
- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими.

«Комплекс 3А»

- включает *аутентификацию* (или идентификацию), *авторизацию* и *администрирование*. Идентификация и авторизация – это ключевые элементы информационной безопасности.

- При попытке доступа к информационным активам функция *идентификации* дает ответ на вопросы: «Кто вы?» и «Где вы?» – являетесь ли вы авторизованным пользователем сети.
- Функция *авторизации* отвечает за то, к каким ресурсам конкретный пользователь имеет доступ.
- Функция *администрирования* заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Аутентификация

Один из способов аутентификации в компьютерной системе состоит во вводе пользовательского идентификатора, в просторечии называемого «логином» (англ. *login* – регистрационное имя пользователя) и пароля – некой конфиденциальной информации, знание которой обеспечивает владение определенным ресурсом.

Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных и, в случае совпадения, пропускает пользователя в систему.

Конфиденциальность

- Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам.
- Основные требования, предъявляемые к системам шифрования, – высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Межсетевой экран

- представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

Основной принцип действия межсетевых экранов – проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов.

Средства контентной фильтрации

Фильтрация содержимого входящей и исходящей электронной почты, проверка самих почтовых сообщений и вложений в них на основе правил, установленных в организации, позволяет обезопасить компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические.

Проверка целостности содержимого дисков

Все изменения на рабочей станции или на сервере могут быть отслежены администратором сети или другим авторизованным пользователем благодаря технологии проверки целостности содержимого жесткого диска (integrity checking).

Это позволяет обнаруживать любые действия с файлами (изменение, удаление или же просто открытие) и идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями. Контроль осуществляется на основе анализа контрольных сумм файлов (CRC-сумм).

Современные антивирусные технологии

- позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие практически под любой из распространенных операционных систем (Windows, Unix и Linux, Novell) на процессорах различных типов.

Основные признаки появления вируса в компьютере:

- неожиданная неработоспособность компьютера или его компонентов;
- невозможность загрузки операционной системы;
- медленная работа компьютера;
- частые зависания и сбои в компьютере;
- прекращение работы ранее успешно исполнявшихся программ;
- искажение или исчезновение файлов и каталогов;
- непредусмотренное форматирование диска;
- необоснованное увеличение количества файлов на диске;
- необоснованное изменение размера файлов;
- искажение данных в CMOS-памяти;
- существенное уменьшение объема свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений и изображений;
- появление непредусмотренных звуковых сигналов.

Антивирусные программы

- программы-детекторы;
- программы-ревизоры,
- программы-фильтры;
- программы-доктора, или дезинфекторы, фаги;
- программы-вакцины, или иммунизаторы.

Программы-детекторы

- осуществляют поиск компьютерных вирусов в памяти машины и при их обнаружении сообщают об этом. Детекторы могут искать как уже известные вирусы (ищут характерную для конкретного уже известного вируса последовательность байтов - сигнатуру вируса), так и произвольные вирусы (путем подсчета кон трольных сумм для массива файла).

Программы-ревизоры

- Являются развитием детекторов, но выполняют более сложную работу. Они запоминают исходное состояние программ, каталогов, системных областей и периодически или по указанию пользователя сравнивают его с текущим.
- При сравнении проверяется длина файлов, дата их создания и модификации, контрольные суммы и байты циклического контроля и другие параметры.
- Ревизоры эффективнее детекторов.

Программы-фильтры

- Обеспечивают выявление подозрительных, характерных для вирусов действий (коррекция исполняемых .exe и .com файлов, запись в загрузочные секторы дисков, изменение атрибутов файлов, прямая запись на диск по прямому адресу и т.д.).
- При обнаружении таких действий фильтры посылают пользователю запрос о подтверждении правомерности таких процедур.

Программы-доктора

Самые распространенные и популярные (например, Kaspersky Antivirus, Doctor Web, Norton Antivirus и т. д.), которые не только обнаруживают, но и лечат зараженные вирусами файлы и загрузочные секторы дисков.

Они сначала ищут вирусы в оперативной памяти и уничтожают их там (удаляют тело резидентного файла, а затем лечат файлы и диски). Многие программы-доктора являются полифагами и обновляются достаточно часто.

Программы-вакцины

Применяются для предотвращения заражения файлов и дисков известными вирусами. Вакцины модифицируют файл или диск таким образом, что он воспринимается программой-вирусом уже зараженным, и поэтому вирус не внедряется.

ДЛЯ защиты компьютера от вирусов необходимо:

- не использовать нелицензионные или непроверенные программные продукты;
- иметь на компьютере один или несколько наборов антивирусных программ и обновлять их еженедельно;
- не пользоваться дисками с чужих компьютеров, а при необходимости такого использования сразу же проверять их антивирусными программами;
- не запускать программ, назначение которых неизвестно или непонятно;
- использовать антивирусные программы для входного контроля информации, поступающей по сети;
- не раскрывать вложения в электронные письма от неизвестных отправителей;
- при переносе на компьютер архивированных файлов сразу же после разархивирования проверять их антивирусными программами;
- перед открытием текстовых, табличных и иных файлов, содержащих макросы, проверять их на наличие вирусов;
- периодически проверять винчестер на наличие вирусов;
- не оставлять диски в дисководе при включении и выключении компьютера во избежание заражения их загрузочными вирусами.

- Системы обнаружения уязвимостей компьютерных сетей и анализаторы сетевых атак безопасно моделируют распространенные атаки и способы вторжения и определяют, что именно хакер может увидеть в сети и как он может использовать ее ресурсы.
- Резервное копирование – один из основных методов защиты от потери данных с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т.д.).

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- *Криптографическое закрытие информации* выполняется путем преобразования информационного сообщения, первоначально открытого и незащищенного, по специальному алгоритму с использованием процедур *шифрования*, в результате чего невозможно определить содержание данных, не зная ключа.
- В таком виде сообщение передается по каналу связи, даже и не защищенному. Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

На практике используется два типа шифрования:

- симметричное
- асимметричное

Симметричное шифрование

- При симметричном шифровании для *шифрования* и *дешифрования* данных используется один и тот же секретный ключ.
- При этом сам ключ должен быть передан безопасным способом участникам взаимодействия до начала передачи зашифрованных данных.

- Если ключ стал известен третьему лицу, то последнее, используя этот ключ, имеет возможность перехватить сообщение и подменить его своим собственным, а затем, получив доступ ко всей информации, передаваемой между абонентами, использовать ее в корыстных целях.
- Для защиты от подобных событий можно использовать систему цифровых сертификатов, то есть документов, выдаваемых сертификационной службой и содержащих информацию о владельце сертификата, зашифрованную с помощью закрытого ключа этой организации. Запросив такой сертификат, абонент, получающий информацию, может удостовериться в подлинности сообщения.

Асимметричное шифрование (система с открытым ключом)

- Является наиболее перспективной системой криптографической защиты данных.
- для шифрования и дешифрования используются разные ключи, которые связаны между собой. Знание одного ключа не позволяет определить другой.
- Один ключ свободно распространяется и является **открытым** (*public key*), второй ключ известен только его владельцу и является **закрытым** (*private key*).
- Знание открытого ключа не позволяет определить ключ секретный.

- Если шифрование выполняется открытым ключом, то сообщение может быть расшифровано только владельцем закрытого ключа - такой метод шифрования используется для передачи конфиденциальной информации.
- Если сообщение шифруется закрытым ключом, то оно может быть расшифровано любым пользователем, зна ющим открытый ключ, но изменить или подменить зашифрованное сообщение так, чтобы это осталось незамеченным, владелец открытого ключа не может.
- Этот метод шифрования предназначен для пересылки открытых документов, текст которых не может быть изме нен.
- Криптостойкость асимметричного шифрования обеспечивается сложной комбинаторной задачей, решить которую методом полного перебора не представляется возможным.

Электронная цифровая подпись

- Электронная подпись отвечает за достоверность электронного документа. Это более современный аналог обычной подписи, которой удостоверяется бумажная документация.
- ЭЦП может быть включена в тело отправляемого файла или приложена отдельно.
- ЭЦП состоит из уникальной последовательности символов, полученной в результате криптографического преобразования исходной информации с использованием закрытого ключа и позволяющая подтверждать целостность и неизменность этой информации, а также ее авторство путем применения открытого ключа.
- Эта последовательность может иметь разные степени защиты, от которых зависят возможности применения ЭЦП.

С использованием ЭЦП можно:

- повысить конфиденциальность информационного обмена документами;
- сократить до нескольких секунд время отправки подписанных документов;
- упростить участие в электронных торгах и сдачу отчетности в государственные контролирующие органы;
- гарантировать достоверность документации;
- участвовать в международном документообороте;
- повысить эффективность корпоративного документооборота.

Виды электронной подписи:

- *Простая электронная подпись*. Этот вид подписи удостоверяет, что электронный документ был отправлен именно вами.
- *Усиленная неквалифицированная электронная подпись* подтверждает, что в документ с момент его подписания не вносились изменения.
- *Усиленная квалифицированная электронная подпись* юридически приравнивается к бумажному документу с «живой» подписью.

- В последнее чаще используется наиболее защищенная и дающая больше возможностей усиленная квалифицированная подпись.
- Для ее использования выдается два ключа: закрытый и открытый, которые работают только в паре.

- *Закрытый ключ* представляет собой 256 бит кодированной информации, а открытый – 1024 бита.
- *Открытый ключ* при помощи специального сертификата вы должны будете предоставить всем, с кем вы хотите обмениваться документами.
- *Сертификат электронной подписи* удостоверяет вашу личность. В целях защиты от подделок и искажений дубликат открытого ключа хранится в библиотеке *Удостоверяющего Центра*. Закрытый ключ позволяет вам осуществлять подписание документов и отсылку сертификата. Благодаря ему, эти операции доступны только вам. Сертификат имеет срок действия, не превышающий 365 дней. По окончании этого срока требуется получение нового сертификата.

- Подделка ЭЦП любого из трех видов невозможна, поскольку для этого потребовались бы колоссальные вычисления, крайне затратные по времени даже при современном уровне развития вычислительной техники. По желанию владельца, его ЭЦП может быть застрахована.

- Для получения ЭЦП необходимо подать заявку в сертифицированный удостоверяющий центр, приложив комплект документов.

Проверка электронной подписи

- Для проверки электронной подписи существует ряд специальных программ, которые можно установить на ваш компьютер или использовать онлайн.
- Как правило, подобную программу предлагает сертифицированный удостоверяющий центр, где оформляется ЭЦП.
- Для проверки на подлинность ЭЦП извлекается из документа или письма и загружается в программу. Высокопроизводительные программы позволяют проверять целые папки документов, экономя время.

- Следи за собой: почему начинается эпидемия воровства данных
- Наталья Касперская
  Генеральный директор компании InfoWatch
  http://www.rbc.ru/opinions/technology_and_media/23/09/2015/5602b2939a794730bc72ffa9

- Аналитический центр InfoWatch опубликовал новое исследование утечек конфиденциальной информации.
- Россия оказалась на втором месте в мире после США.

Как правило, информацию об утечках компании скрывают, поэтому анализируем только те случаи, о которых стало известно прессе, - *за первое полугодие 2015 года их было 723.*

Нужно оговориться, что наши исследователи изучают информацию о краже данных в русскоязычных и англоязычных источниках, на это надо делать поправку. Не исключено, что, например, в Китае воруют чаще, но мы узнаем об этих инцидентах реже.

Что воруют?

- Чаще всего информацию у компаний крадут собственные сотрудники (в 65% случаев в утечке был виновен персонал). А в период сокращений и массовых увольнений у многих сотрудников появляется мотив что-то унести. Данные, как правило, украсть проще, чем что-то материальное.

- Самый распространенный объект для воровства - это персональные данные, почти 90% случаев.
- Чаще всего люди сливают базы данных - они ликвидны, на них легко найти покупателя.
- Можно их продать на открытом рынке (в интернете или по старинке на «Горбушке»), можно предложить новому работодателю, можно открыть собственное дело. У россиян такая ментальность, что базы данных клиентов продавцы зачастую считают своей личной собственностью и не испытывают угрызений совести.

- Значительная часть краж персональных данных в западных странах приходится на медицинские учреждения.
- Людям таргетировано предлагают лекарства, врачей, услуги клиник.
- В России злоумышленников интересуют в первую очередь данные клиентов банков. Кредитные учреждения в системном кризисе и не брезгуют никакими методами, чтобы переманить клиентов.
- Незначительная доля утечек приходится на мошенников, которые воруют с помощью этих данных деньги. Зачастую спамерские рассылки — это результат утечки данных.

- Немногим более 5% утечек — это коммерческая тайна, разработки и ноу-хау.
- Чуть меньше, порядка 3%, — сведения, составляющие государственную тайну. Но масштаб и значимость таких утечек как минимум не ниже.

Как воруют?

- Зарегистрировано 22 мегаутечки, в ходе которых были украдены данные более 1 млн записей.
- Это означает, что в открытый доступ попала персональная информация более 1 млн человек.
- Страдают все - от сенаторов до абонентов сотовой связи.
- Причем утечки происходят как в сегменте крупных предприятий, так и в компаниях среднего и малого бизнеса.

- Традиционно популярный инструмент воровства - это обычный принтер.
- Часто компании считают, что нужно защищать в первую очередь электронную почту. Но сотрудники просто распечатывают информацию и уносят домой. Поэтому нужно отслеживать и те потоки данных, которые отправляются на принтер.

- Согласно последней статистике, основным каналом утечек информации становится Сеть. Это связано с развитием облачных технологий. Люди напрямую загружают в Dropbox данные — и все, прощай информация.

- Также распространено хищение устройств — ноутбуков, смартфонов. Их воруют, забывают. В России много таких историй.

Что дальше?

- Вектор развития очевиден — с каждым годом количество утечек растет на 10–15%.
- В России сейчас рост еще более динамичный.
- Проблема в том, что защита от утечек — это более сложная задача, чем защита от вирусов. С вирусами работает бинарная логика — программа определяет, вирус перед ней или нет. С данными это не так. Мы боремся с внутренними нарушителями. Нельзя взять и запретить людям обмениваться электронными сообщениями или печатать документы. Программа должна уметь определять степень конфиденциальности информации, перехватывать именно те данные, которые нужно защищать. Поэтому создать 100-процентную защиту невозможно.

- Главное отличие российского бизнеса в деле защиты информации - это «пофигизм». Большинство компаний не знают, какую информацию надо защищать, как это делать и зачем.
- Уровень системных администраторов у нас даже выше, чем в других странах, например в ЕС, но при этом они зачастую или недооценивают степень угрозы, или пытаются решить проблему собственными методами.
- Многие настроены на авось - пронесет или не пронесет.

- Самый защищенный сектор - банковский. Около 50% банков борются с утечками.
- В производственном секторе - только 10–20%. Более того, многие начинают экономить на защите.