Содержание:

Введение

Сегодня я расскажу Вам о том, как нужно поддерживать уровень своей информационной безопасности.

Каждый человек хотя бы раз в жизни слышал о необходимости поддерживать уровень своей информационной безопасности. Все слышали советы на тему обеспечения безопасности, но вот только толку от них почему-то получается не очень много. Во многом причина заключается в отсутствии понимании таких вещей, как "что мы защищаем", "от кого мы это защищаем" и "что хотим получить в конце". Сегодня я расскажу Вам об этом.

1: Понятие информационной безопасности

«Информационная безопасность» - этот термин подразумевает под собой различные меры, состояния сохранности, технологий и прочее, однако все не так уж и сложно, как Вы думаете. И я бы хотела задать Вам вопрос «сколько человек из вашего окружения хотя бы прочитало определение этого понятия, а не просто подразумевает сопоставление слов с их значениями?» Большинство людей ассоциируют безопасность с антивирусами, и другими программами безопасности. Да, программы безопасности защитят ваш компьютер от угроз и повысят уровень защитной системы, но что на самом деле делают эти программы, знает малое количество людей.

Появление любых новых технологий, имеет как положительную, так и отрицательную сторону. Есть множество примеров этому:

Интенсивное развитие транспорта обеспечило быструю и удобную доставку людей, материалов и товаров в нужных направления, но также и материальный ущерб, и человеческие жертвы при транспортных катастрофах стало больше.

Информационные технологии, тоже не являются исключением из этого списка, и поэтому людям следует заранее позаботиться о безопасности при разработке и использовании таких технологий.

От безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей.

2. Основные угрозы информационной безопасности

Информационная система — это система, состоящая из большого количества компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Каждый компонент может выйти из строя. Компоненты автоматизированной информационной системы можно поделить на следующие группы:

- аппаратные средства - компьютеры и их составные части.
- программное обеспечение - приобретенные программы, исходные, загрузочные модули; операционные системы и системные программы утилиты, диагностические программы и т.д.
- данные, хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.
- персонал - обслуживающий персонал и пользователи.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия — это уже целенаправленные действие. Нарушителем может быть любой человек, который хочет заполучить информацию, то есть это может быть ваш коллега, конкуренты, и т.д.

Действия нарушителя могут быть обусловлены разными мотивами:

- недовольством своей должностью;
- взяткой;
- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы.

Нарушитель выбирает наиболее слабое звено в защите.

3.Обеспечение информационной безопасности

Обеспечение информационной безопасности **-** часто приравнивают к техническим решениям, оставляя без внимания потенциал угроз, как действия самого человека.

Чтобы определиться с защитой ваших данных, необходимо не только искать подходящие средства безопасности, но и задумываться о том, как информация может распространяться и чего она может касаться. Для примера, можно взять задачу сохранить пароль в тайне, насколько это возможно?

Представьте: Вы придумали пароль, очень сложный пароль, никак не связанный с вами, или с вашими близкими. Он полностью соответствующий самым жестким требованиям безопасности. Для того, чтобы ваши данные не взломали вам надо будет постоянно вводить пароль только с одного компьютера, используя безопасную клавиатуру. Для соединения используете только VPN, компьютер загружаете только с LiveCD. Однако, этого всего может быть недостаточно для защиты пароля.

Вот вам несколько простых ситуаций, демонстрирующих необходимость в широком взгляде на методы защиты информации:

1: что вы будете делать, если вам нужно ввести пароль, когда в комнате присутствуют другие люди, пусть даже ваши лучшие друзья? Вы никогда не сможете гарантировать, что они случайным образом не обмолвятся о косвенной информации о пароле.

2: что вы будете делать, если так случилось и вам нужно, чтобы за вас осуществил операцию другой человек? Пароль может случайно услышать другой человек, и спокойно взломать вашу систему.

3: как вы сможете защитить пароль, если один из узлов, обеспечивающих безопасную передачу пароля, был взломан злоумышленником?

4: будет ли иметь смысл ваш пароль, если используемая система была взломана?

Я не говорю о том, что надо сидеть месяцами и искать очень хорошую защиту информации. Речь идет о том, что даже самые сложные системы могут быть взломаны простыми человеческим способом, рассмотрение которых было заброшено. Поэтому, занимаясь обустройством безопасности вашего компьютера, старайтесь уделять внимание не только технической стороне вопроса, но и окружающему вас миру.

4.Аппаратно-программные средства защиты информации

Несмотря на то, что современная ОС для персональных компьютеров, имеет собственные подсистемы защиты, создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно поделить на 5 групп:

1: системы идентификации и аутентификации пользователей.

2: системы шифрования дисковых данных.

3: системы шифрования данных, передаваемых по сетям.

4: системы аутентификации электронных данных.

5: средства управления криптографическими ключами.

4. 1. Системы идентификации и аутентификации пользователей

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам вашей компьютерной системы. Работа такой системы заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить этому пользователю возможность работы с системой.

При построении этих систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

- секретная информация, которой обладает только пользователь.
- физиологические параметры человека, или особенности поведения.

Системы, основанные на первом типе информации, считаются традиционными. Системы, использующие второй тип информации, называют биометрическими.

4. 2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая криптографией.

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать

криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt. Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования. По способу функционирования системы шифрования дисковых данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

Большинство систем, предлагающих установить пароль на документ, не шифрует информацию, а только обеспечивает запрос пароля при доступе к документу. К таким системам относится MS Office, 1С и многие другие. **4. 3. Системы шифрования данных, передаваемых по сетям**

Различают два основных способа шифрования: канальное шифрование и оконечное шифрование.

В случае канального шифрования защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством: встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

1: шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации.

2: шифрование служебной информации может привести к появлению статистических закономерностей в шифрованных данных, что влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся остальная информация остается открытой. Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

4. 4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения или электронную подпись.

Имтовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имтовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Таким образом, для реализации имтовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного.

4. 5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Существуют следующие виды функций управления ключами: генерация, хранение, и распределение ключей.

Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.

Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ ключ шифрования ключей и ключ шифрования данных.

Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.

Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

Заключение

Я рассказала Вам о «Информационной безопасности и защиты информации».

Какой можно теперь можно сделать из этого вывод?

То, что информация — это ресурс, и потеря конфиденциальной информации приносит моральный или материальный ущерб. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и т.д. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Источники

1: https://ru.wikipedia.org/wiki/Информационная_безопасность

2: Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. – 544 с.

3: информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с.

4: из источников собственных знаний.