Методы и приемы обеспечения информационной безопасности

Под безопасностью информации (Information security) **или информационной безопасностью** понимают защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей её структуре.

При рассмотрении проблем, связанных с обеспечением безопасности, используют понятие «**несанкционированный доступ**» – это неправомочное обращение к информационным ресурсам с целью их использования (чтения, модификации), а также порчи или уничтожения. Данное понятие также связано с распространением разного рода компьютерных вирусов.

В свою очередь «**санкционированный доступ**» – это доступ к объектам, программам и данным пользователей, имеющих право выполнять определённые действия (чтение, копирование и др.), а также полномочия и права пользователей на использование ресурсов и услуг, определённых администратором вычислительной системы.

Вирусы представляют широко распространённое явление, отражающееся на большинстве пользователей компьютеров, особенно работающих в сетях и с нелицензионным программным обеспечением.

Вирусы появились в результате создания самозапускающихся программ.

Вирусы – это класс программ, незаконно проникающих в компьютеры пользователей и наносящих вред их программному обеспечению, информационным файлам и даже техническим устройствам, например, жёсткому магнитному диску. В России вирусы появляются в 1988 году. С развитием сетевых информационных технологий вирусы стали представлять угрозу огромному количеству пользователей сетевых и локальных компьютерных систем.

Основные средства и методы защиты информации

Средства и методы защиты информации обычно делят на две большие группы: организационные и технические.

Под организационными подразумеваются законодательные, административные и физические, а **под техническими** – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, людей и информации.

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

С целью организации защиты объектов используют **системы охраны** и **безопасности объектов** – это совокупность взаимодействующих радиоэлектронных приборов, устройств и электрооборудования, средств технической и инженерной защиты, специально подготовленного персонала, а также транспорта, выполняющих названную функцию. При этом используются различные методы, обеспечивающие санкционированным лицам доступ к объектам и ИР. К ним относят аутентификацию и идентификацию пользователей.

Программные и технические средства защиты.

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Программные средства защиты представляют комплекс алгоритмов и программ специального назначения и общего обеспечения работы компьютеров и информационных сетей. Они нацелены на: контроль и разграничение доступа к информации, исключение несанкционированных действий с ней, управление охранными устройствами и т.п. Программные средства защиты обладают универсальностью, простотой реализации, гибкостью, адаптивностью, возможностью настройки системы и др

Широко применяются программные средства для защиты от компьютерных вирусов.

Для **защиты машин от компьютерных вирусов**, профилактики и «лечения» используются программы-антивирусы, а также средства диагностики и профилактики, позволяющие не допустить попадания вируса в компьютерную систему, лечить заражённые файлы и диски, обнаруживать и предотвращать подозрительные действия. Антивирусные программы оцениваются по точности обнаружения и эффективному устранение вирусов, простое использование, стоимость, возможности работать в сети.

Наибольшей популярностью пользуются программы, предназначенные для профилактики заражения, обнаружения и уничтожения вирусов. Среди них отечественные антивирусные программы DrWeb (Doctor Web) И. Данилова и AVP (Antiviral Toolkit Pro) Е. Касперского. Они обладают удобным интерфейсом, средствами сканирования программ, проверки системы при загрузке и т.д. В России используются и зарубежные антивирусные программы. Абсолютно надёжных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Только многоуровневая оборона способна обеспечить наиболее полную защиту от вирусов. Важным элементом защиты от компьютерных вирусов является профилактика. Антивирусные программы применяют одновременно с регулярным резервированием данных и профилактическими мероприятиями. Вместе эти меры позволяют значительно снизить вероятность заражения вирусом.

Основными мерами профилактики вирусов являются:

1) применение лицензионного программного обеспечения;

2) регулярное использование нескольких постоянно обновляемых антивирусных программ для проверки не только собственных носителей информации при переносе на них сторонних файлов, но и любых «чужих» дискет и дисков с любой информацией на них, в т.ч. и переформатированных; 3) применение различных защитных средств при работе на компьютере в любой информационной среде (например, в Интернете). Проверка на наличие вирусов файлов, полученных по сети;

4) периодическое резервное копирование наиболее ценных данных и программ. Одним из наиболее известных способов защиты информации является её кодирование (шифрование, криптография). Оно не спасает от физических воздействий, но в остальных случаях служит надёжным средством.

Код характеризуется: *длиной* – числом знаков, используемых при кодировании и структурой – порядком расположения символов, используемых для обозначения классификационного признака.

Средством кодирования служит таблица соответствия. Примером такой таблицы для перевода алфавитно-цифровой информации в компьютерные коды является кодовая таблица ASCII.

Криптографические методы защиты информации.

Криптография - это тайнопись, система изменения информации с целью её защиты от несанкционированных воздействий, а также обеспечения

достоверности передаваемых данных.

Общие методы криптографии существуют давно. Она считается мощным средством обеспечения конфиденциальности и контроля целостности информации. Пока альтернативы методам криптографии нет.

Стойкость криптоалгоритма зависит от сложности методов преобразования. Вопросами разработки, продажи и использования средств шифрования данных и сертификации средств защиты данных занимается Гостехкомиссия РФ.

Одной из важных проблем информационной безопасности является организация защиты электронных данных и электронных документов. Для их кодирования, с целью удовлетворения требованиям обеспечения безопасности данных от несанкционированных воздействий на них, используется электронная цифровая подпись (ЭЦП).

Электронная подпись

Цифровая подпись представляет последовательность символов. Она зависит от самого сообщения и от секретного ключа, известного только подписывающему это сообщение.

Первый отечественный стандарт ЭЦП появился в 1994 году. Вопросами использования ЭЦП в России занимается Федеральное агентство по информационным технологиям (ФАИТ).

Биометрические методы защиты.

Наиболее чётко обеспечивают защиту средства идентификации личности, использующие биометрические системы. Понятие «биометрия» определяет раздел биологии, занимающийся количественными биологическими экспериментами с привлечением методов математической статистики. Это научное направление появилось в конце XIX века.

Биометрия - это совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологических или поведенческих характеристиках.

Биометрические системы позволяют идентифицировать человека по присущим ему специфическим признакам, то есть по его статическим (отпечаткам пальцев, роговице глаза, форме руки и лица, генетическому коду, запаху и др.) и динамическим (голосу, почерку, поведению и др.) характеристикам. Уникальные биологические, физиологические и поведенческие характеристики, индивидуальные для каждого человека. Они называются биологическим кодом человека.

Первые биометрические системы использовали рисунок (отпечаток) пальца. Примерно одну тысячу лет до н.э. в Китае и Вавилоне знали об уникальности отпечатков пальцев. Их ставили под юридическими

документами. Однако дактилоскопию стали применять в Англии с 1897 года, а в США – с 1903 года. Пример современного считывающего устройства отпечатки пальцев

С помощью биометрических систем осуществляются:

1) ограничение доступа к информации и обеспечение персональной ответственности за её сохранность;

2) обеспечение допуска сертифицированных специалистов;

3) предотвращение проникновения злоумышленников на охраняемые территории и в помещения вследствие подделки и (или) кражи документов (карт, паролей);

4) организация учёта доступа и посещаемости сотрудников, а также решается ряд других проблем.

Одним из наиболее надёжных способов считается идентификация глаз человека

: идентификация рисунка радужной оболочки глаза или сканирование глазного дна (сетчатки глаза). Это связано с отличным соотношением точности идентификации и простотой использования оборудования. Изображение радужной оболочки оцифровывается и сохраняется в системе в виде кода. Код, полученный в результате считывания биометрических параметров человека, сравнивается с зарегистрированным в системе. При их совпадении система снимает блокировку доступа. Время сканирования не превышает двух секунд. К новым биометрическим технологиям следует отнести трёхмерную идентификацию личности, использующую трёхмерные сканеры идентификации личности с параллаксным методом регистрации образов объектов и телевизионные системы регистрации изображений со сверхбольшим угловым полем зрения. Предполагается, что подобные системы будут использоваться для идентификации личностей, трёхмерные образы которых войдут в состав удостоверений личности и других документов.

Сетевые методы защиты

Для защиты информации в информационных компьютерных сетях используют специальные программные, технические и программно-технические средства. С целью защиты сетей и контроля доступа в них используют:

- фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;
- фильтрующие маршрутизаторы, реализующие алгоритмы анализа

адресов отправления и назначения пакетов в сети;

- шлюзы прикладных программ, проверяющие права доступа к программам.

В качестве устройства, препятствующего получению злоумышленником доступа к информации, используют **Firewalls** (англ. «огненная стена» или «защитный барьер» – брандмауэр). Такое устройство располагают между внутренней локальной сетью организации и Интернетом. Оно ограничивает трафик, пресекает попытки несанкционированного доступа к внутренним ресурсам организации. Это внешняя защита. Современные брандмауэры могут «отсекать» от пользователей корпоративных сетей незаконную и нежелательную для них корреспонденцию, передаваемую по электронной почте. При этом ограничивается возможность получении избыточной информации и так называемого «мусора» (спама).

Другим техническим устройством эффективной защиты в компьютерных сетях является **маршрутизатор**. Он осуществляет фильтрацию пакетов передаваемых данных. В результате появляется возможность запретить доступ некоторым пользователям к определённому «хосту», программно осуществлять детальный контроль адресов отправителей и получателей. Так же можно ограничить доступ всем или определённым категориям пользователей к различным серверам, например, ведущим распространение противоправной или антисоциальной информации (пропаганда секса, насилия и т.п.).

Защита может осуществляться не только в глобальной сети или локальной сети организации, но и отдельных компьютеров. Для этой цели создаются специальные программно-аппаратные комплексы.

Для комплексной защиты информации, объектов и людей на различных предприятиях рекомендуется разрабатывать и внедрять соответствующие мероприятия.

Общие выводы

Важно знать, что характерной особенностью электронных данных является возможность легко и незаметно искажать, копировать или уничтожать их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию.

Защищённой называют информацию, не изменившую в процессе передачи, хранения и сохранения достоверность, полноту и целостность

данных. Несанкционированные воздействия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью разных методов воздействия. Подобные действия могут быть обусловлены стихийными бедствиями (ураганы, ливни, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с ними обычно весьма затруднена из-за в значительной степени непредсказуемости таких воздействий.

Наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Для защиты информации в компьютерах и информационных сетях широко используются разнообразные программные и программно-технические средства защиты. Они включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения. Для защиты информации от утечки в компьютерных сетях используют специальное техническое средство – **Firewall**s, располагаемое между внутренней локальной сетью организации и Интернетом.

Другим устройством эффективной защиты в компьютерных сетях является **маршрутизатор.** Он осуществляет фильтрацию пакетов передаваемых данных и, тем самым, появляется возможность запретить доступ некоторым пользователям к определённому «хосту», программно осуществлять детальный контроль адресов отправителей и получателей и др.

Охрана и безопасность объектов, людей и информации достигается взаимодействием специальных радиоэлектронных приборов, устройств и электрооборудования, в т.ч. пожарной и охранной сигнализации, средств технической и инженерной защиты, специально подготовленного персонала и транспорта. В качестве технических средств используются решётки на окна, ограждения, металлические двери, турникеты, металодетекторы и др.

К наиболее практикуемым способам защиты информации относится её кодирование, предполагающее использование криптографических методов защиты информации. Оно не спасает от физических воздействий, но в остальных случаях служит надёжным средством. Другой метод предполагает использование устройств, ограничивающих доступ к объектам и данным. Ведущее место среди них занимают биометрические системы. Они позволяют идентифицировать человека по присущим ему специфическим статическим и динамическим признакам (отпечаткам пальцев, роговице глаза, форме руки, лицу, генетическому коду, запаху, голосу, почерку, поведению и др.). Комплексно мероприятия по обеспечению сохранности и защиты информации, объектов и людей включают организационные, физические, социально-психологические мероприятия и инженерно-

технические средства защиты.

Контрольные вопросы.

1. Что такое компьютерный вирус?

2. Назначение компьютерного вируса? 3. Типы вирусов.

4. Программные средства защиты – антивирусные программы (характеристика).

5. Безопасность программно-технических средств и информационных ресурсов (характеристика).

6. Программная защита от несанкционированных воздействий.

7. Криптография, криптографическая защита от несанкционированных воздействий (характеристика).

8. Что такое электронная подпись?

9. Физическая и техническая защита от несанкционированных воздействий (характеристика).

10.Воздействия на здания, помещения, личную безопасность пользователя и обслуживающий персонал.

11.Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации (характеристика).

12. Охрана объектов с целью ограничения свободного доступа, смарткарты и др. (характеристика).