5. Информационные технологии безопасности и защиты

План

1. Общие положения защиты информации
2. Несанкционированные действия и методы воздействия на информацию, здания, помещения и людей
3. Средства и методы защиты информации, зданий, помещений и людей в них
4. Мероприятия по обеспечению сохранности и защиты

1. Общие положения защиты информации

Практически вся современная информация готовится или может быть достаточно легко преобразована в машиночитаемую форму. Характерной особенностью такой информации является возможность посторонних лиц легко и незаметно исказить, скопировать или уничтожить её. Это обстоятельство вызывает необходимость организации безопасного функционирования данных в любых информационных системах. Такие мероприятия называют защитой информации или информационной безопасностью.

Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Подобные воздействия происходят также по причине стихийных бедствий, техногенных катастроф и террористических актов.

Проблемы информационной безопасности имеют не только местные (частные) и государственные, но и геополитические аспекты. Это комплексная проблема, поэтому её решение рассматривается на разных уровнях: законодательном, административном, процедурном и программно-техническом.

Слово “безопасность” латинского происхождения – secure (securus). Затем в английском языке оно получило написание “security”.

Общеизвестно, что “безопасность” – это отсутствие опасности; состояние деятельности, при которой с определённой вероятностью исключено причинение ущерба здоровью человека, зданиям, помещениям и материально-техническим средствам в них.

> Безопасность - это состояние субъекта, или объекта, при котором отсутствует угроза нанесения им какого-либо ущерба.

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.

Защищённой считают информацию, не претерпевшую незаконных изменений в процессе передачи, хранения и сохранения, не изменившую такие свойства, как достоверность, полнота и целостность данных.

Под терминами “защита информации” и “информационная безопасность” подразумевается совокупность методов, средств и мероприятий, направленных на исключение искажений, уничтожения и несанкционированного использования накапливаемых, обрабатываемых и хранимых данных.

В законе “Об информации, информатизации и защите информации” (ст. 20) определено, что целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокировке информации.

2. Несанкционированные действия и методы воздействия на информацию, здания, помещения и людей

Несанкционированные действия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью различных 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.

Однако наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Американские специалисты утверждают, что до 85% случаев промышленного шпионажа ведётся силами сотрудников компании, в которой это происходит. В 2004 г. более трети финансовых потерь и потерь данных в организациях происходило по вине их собственных сотрудников. Решение этих проблем относится к компетенции администрации и службы безопасности организации. При этом рекомендуется шифровать даже внутрифирменную переписку.

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

Компьютерный вирус - это специальная, способная к саморазмножению программа, обычно составляемая со злым умыслом.

Вирусы появились в результате создания самозапускающихся программ. Внешняя схожесть этих программ с биологией и медициной по характеру воздействия на программно-технические средства способствовала появлению таких терминов, как: вирус, заражение, лечение, профилактика, прививки, доктор и др. Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется заражением, а программа или иной объект, содержащий вирус – заражёнными.

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.

Вирусы проникают и в карманные персональные компьютеры (КПК) Первая троянская программа для КПК (Backdoor.WinCE.Brador.a – утилита скрытого дистанционного доступа) обнаружена в августе 2004 года. Она может добавлять, удалять файлы на КПК, а также пересылать их автору вируса.

Программа-вирус обычно состоит из уникальной последовательности команд – сигнатур (знаков) и поведений, что позволяет создавать обнаруживающие их программы-антивирусы. Некоторые вирусы не имеют уникальных сигнатур и поведения и могут видоизменять самих себя (полиморфные).

По утверждению специалистов, заражение вирусами компьютеров составляет лишь доли процентов там, где работают, а не играют. Всё большую роль в области несанкционированных воздействий на информацию, здания, помещения, личную безопасность пользователя и обслуживающий персонал играют ошибочные (в т. ч. случайные) и преднамеренные действия людей.

Типичными причинами нарушения безопасности на объекте являются:

1) ошибки индивидов или неточные их действия;

2) неисправность и (или) отказ используемого оборудования;

3) непредсказуемые и недопустимые внешние проявления;

4) неисправность и (или) отсутствие необходимых средств защиты;

5) случайные и преднамеренные воздействия на информацию, защищаемые элементы оборудования, человека и окружающую среду.

Установлено, что ошибочные действия людей составляют 50–80% , а технических средств – 15–25% нарушений безопасности объектов и данных. Ошибочные и несанкционированные действия людей объясняются недостаточной их дисциплинированностью и подготовленностью к работе, опасной технологией и несовершенством используемой ими техники. Известно, что число связанных с человеческим фактором техногенных аварий и катастроф доходит до двух третей от общего их количества.

Отрицательное воздействие на человека оказывает не только незащищённость информации, но и стихийные бедствия, последствия техногенных влияний на природу, нарушения правил техники безопасности, террористические акты и другие события, приводящие, в первую очередь, к стрессовым ситуациям. Отрицательные информационные социально-психологические воздействия, в том числе дискомфорт, человек получает и в процессе работы с огромными массивами данных. Кроме стресса, он становится жертвой информационных перегрузок, информационного шума и т.п.

3. Средства и методы защиты информации, зданий, помещений и людей в них

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.

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.

Аутентификация – это метод независимого от источника информации установления подлинности информации на основе проверки подлинности её внутренней структуры (“это тот, кем назвался?”).

Авторизация – в информационных технологиях это предоставление определённых полномочий лицу или группе лиц на выполнение некоторых действий в системе обработки данных. (“имеет ли право выполнять данную

деятельность?”). Посредством авторизации устанавливаются и реализуются права доступа к ресурсам.

Идентификация – это метод сравнения предметов или лиц по их характеристикам, путём опознавания по предметам или документам, определения полномочий, связанных с доступом лиц в помещения, к документам и т. д. (“это тот, кем назвался и имеет право выполнять данную деятельность?”).

В современных информационных технологиях для эффективного использования этих методов, кроме физических мер охраны объектов, широко применяются программно-технические средства, основанные на использовании биометрических систем, криптографии и др.

Эффективность защиты информации в значительной степени зависит от своевременности обнаружения и исключения воздействий на неё, а, при необходимости, восстановления программ, файлов, информации, работоспособности компьютерных устройств и систем. Важной составляющей выполнения подобные действия являются 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.

Чаще всего источниками заражения являются компьютерные игры, приобретенные “неофициальным” путём и нелицензионные программы. Поэтому надёжной гарантией от вирусов является аккуратность пользователей при выборе программ и установке их на компьютер, а также во время сеансов в Интернете. Вероятность заражения не из компьютерной сети можно свести почти к нулю, если пользоваться только лицензионными, легальными продуктами и никогда не пускать на свой компьютер приятелей с неизвестными программами, особенно играми. Наиболее эффективной мерой в этом случае является установление разграничения доступа, не позволяющего вирусам и дефектным программам вредоносно воздействовать на данные даже в случае проникновения вирусов в такой компьютер.

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.

Первый стандарт шифрования появился в 1977 году в США. Главным критерием стойкости любого шифра или кода являются имеющиеся вычислительные мощности и время, в течение которого можно их расшифровать. Если это время равняется нескольким годам, то стойкость таких алгоритмов достаточна для большинства организаций и личностей. Для шифрования информации всё чаще используют криптографические методы её защиты.

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.

Если использовать 256 и более разрядные ключи, то уровень надёжности защиты данных составит десятки и сотни лет работы суперкомпьютера. Для коммерческого применения достаточно 40-, 44-разрядных ключей.

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).

Внедрением в жизнь всех необходимых мероприятий по защите людей, помещений и данных занимаются высококвалифицированные специалисты. Они составляют основу соответствующих подразделений, являются заместителями руководителей организаций и т.п.

Существуют и технические средства защиты.

Технические средства защиты

Технические средства защиты используются в различных ситуациях, входят в состав физических средств защиты и программно-технических систем, комплексов и устройств доступа, видеонаблюдения, сигнализации и других видов защиты.

В простейших ситуациях для защиты персональных компьютеров от несанкционированного запуска и использования имеющихся на них данных предлагается устанавливать устройства, ограничивающие доступ к ним, а также работать со съёмными жёсткими магнитными и магнитооптическими дисками, самозагружающимися компакт дисками, флеш-памятью и др.

Для охраны объектов с целью защиты людей, зданий, помещений, материально-технических средств и информации от несанкционированных воздействий на них, широко используют системы и меры активной безопасности. Общепринято для охраны объектов применять системы управления доступом (СУД). Подобные системы обычно представляют собой автоматизированные системы и комплексы, формируемые на основе программно-технических средств.

В большинстве случаев для защиты информации, ограничения несанкционированного доступа к ней, в здания, помещения и к другим объектам приходится одновременно использовать программные и технические средства, системы и устройства.

Антивирусные программно-технические средства

В качестве технического средства защиты применяют различные электронные ключи, например, HASP (Hardware Against Software Piracy), представляющие аппаратно-программную систему защиты программ и данных от нелегального использования и пиратского тиражирования (Рис. 5.1). Электронные ключи Hardlock используются для защиты программ и файлов данных. В состав системы входит собственно Hardlock, крипто-карта для программирования ключей и программное обеспечение для создания защиты приложений и связанных с ними файлов данных.

К основным программно-техническим мерам, применение которых позволяет решать проблемы обеспечения безопасности ИР, относятся:

- аутентификация пользователя и установление его идентичности;
- управление доступом к БД;
- поддержание целостности данных;
- защита коммуникаций между клиентом и сервером;
- отражение угроз, специфичных для СУБД и др.

Поддержание целостности данных подразумевает наличие не только программно-аппаратных средств поддержки их в рабочем состоянии, но и

мероприятия по защите и архивированию ИР, дублированию их и т.п. Наибольшую опасность для информационных ресурсов, особенно организаций, представляет несанкционированное воздействие на структурированные данные – БД. В целях защиты информации в БД важнейшими являются следующие аспекты информационной безопасности (европейские критерии):

- условия доступа (возможность получить некоторую требуемую информационную услугу);
- целостность (непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Под доступностью понимают обеспечение возможности доступа авторизованных в системе пользователей к информации в соответствии с принятой технологией.

Конфиденциальность – обеспечение пользователям доступа только к данным, для которых они имеют разрешение на доступ (синонимы – секретность, защищённость).

Целостность – обеспечение защиты от преднамеренного или непреднамеренного изменения информации или процессов её обработки.

Эти аспекты являются основополагающими для любого программно-технического обеспечения, предназначенного для создания условий безопасного функционирования данных в компьютерах и компьютерных информационных сетях.

Контроль доступа – это процесс защиты данных и программ от их использования объектами, не имеющими на это права.

Управление доступом служит для контроля входа/выхода работников и посетителей организации через автоматические проходные (турникеты – Рис. 5.2, арочные металодетекторы – Рис. 5.3). Контроль их перемещения осуществляется с помощью систем видеонаблюдения. В управление доступом входят устройства и (или) системы ограждения для ограничения входа на территорию (охрана периметров). Используются также методы визуализации (предъявление вахтёру соответствующих документов) и автоматической идентификации входящих/выходящих работников и посетителей.

Арочные металодетекторы способствуют выявлению несанкционированного вноса/выноса металлизированных предметов и маркированных документов.

Автоматизированные системы управления доступом позволяют работникам и посетителям, пользуясь персональными или разовыми электронными пропусками, проходить через проходную здания организации, заходить в разрешённые помещения и подразделения. Они используют контактный или бесконтактный способ идентификации.

К мерам, обеспечивающим сохранность традиционных и нетрадиционных носителей информации и, как следствие, самой информации относят технологии штрихового кодирования. Эта известная технология широко используется при маркировке различных товаров, в том числе документов, книг и журналов.

В организациях применяют удостоверения, пропуска, читательские билеты и т.п., в том числе в виде пластиковых карт (Рис. 5.4) или ламинированных карточек (Ламинирование - это плёночное покрытие документов, защищающее их от лёгких механических повреждений и загрязнения.), содержащих идентифицирующие пользователей штрих-коды.

Для проверки штрих-кодов используют сканирующие устройства считывания бар-кодов – сканеры. Они преобразуют считанное графическое изображение штрихов в цифровой код. Кроме удобства, штрих-коды обладают и отрицательными качествами: дороговизна используемой технологии, расходных

материалов и специальных программно-технических средств; отсутствие механизмов полной защиты документов от стирания, пропажи и др.

За рубежом вместо штрих-кодов и магнитных полос используют радиоидентификаторы RFID (англ. “Radiofrequency Identification”).

С целью предоставления возможности людям проходить в соответствующие здания и помещения, а также пользоваться информацией применяют контактные и бесконтактные пластиковые и иные магнитные и электронные карты памяти, а также биометрические системы.

Первые в мире пластиковые карточки со встроенными в них микросхемами появились в 1976 году. Они представляют персональное средство аутентификации и хранения данных, аппаратно поддерживают работу с цифровыми технологиями, включая электронную цифровую подпись. Стандартно карта имеет размер 84х54 мм. В неё можно встроить магнитную полосу, микросхему (чип), штрих-код, голограмму, необходимые для автоматизации процессов идентификации пользователей и контроля их доступа на объекты.

Пластиковые карточки используются как бэйджи, пропуска (Рис. 5.4), удостоверения, клубные, банковские, дисконтные, телефонные карты, визитки, календари, сувенирные, презентационные карточки и др. На них можно нанести фотографию, текст, рисунок, фирменный знак (логотип), печать, штрих-код, схему (например, расположения организации), номер и другие данные.

Для работы с ними используют специальные устройства, позволяющие надёжно идентифицировать личность – считыватели смарткарт. Считыватели обеспечивают проверку идентификационного кода и передачу его в контроллер. Они могут фиксировать время прохода или открывания дверей и др.

В качестве идентификаторов широко используются малогабаритные пульты-ключи типа Touch Memory. Эти простейшие контактные устройства обладают высокой надёжностью.

Устройства Touch Memory – специальная малогабаритная (размером с батарейку в виде таблетки) электронная карта в корпусе из нержавеющей стали. Внутри неё расположена микросхема с электронной памятью для установления уникального номера длиной в 48 бит, а также хранения Ф.И.О. пользователя и другой дополнительной информации. Такую карту можно носить на брелке с ключами (рис. 5.5) или разместить на пластиковой карточке сотрудника. Подобные устройства используются в домофонах для осуществления беспрепятственного открытия двери подъезда или помещения. В качестве бесконтактных идентификаторов используют устройства “Proximity”.

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.

Преимущество биологических систем идентификации, по сравнению с традиционными (например, PIN-кодовыми, доступом по паролю), заключается в идентификации не внешних предметов, принадлежащих человеку, а самого человека. Анализируемые характеристики человека невозможно утерять, передать, забыть и крайне сложно подделать. Они практически не подвержены износу и не требуют замены или восстановления. Поэтому в различных странах (в том числе России) включают биометрические признаки в загранпаспорта и другие идентифицирующие личности документы.

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 получения 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.

4. Мероприятия по обеспечению сохранности и защиты

Комплексно мероприятия по обеспечению сохранности и защиты информации, объектов и людей включают организационные, физические, социально-психологические мероприятия и инженерно-технические средства защиты.

Организационные мероприятия предполагают объединение всех составляющих безопасности. Во всём мире основную угрозу информации организации представляют её сотрудники, оказывающиеся психически неуравновешенными, обиженными или неудовлетворенными характером их работы, заработной платой, взаимоотношениями с коллегами и руководителями.

Социально-психологические мероприятия также относятся к организационным. Они включают регулярное проведение организационных мероприятий по недопущению отрицательных воздействий и явлений, по созданию работникам комфортных условий и нормального психологического климата. С этой целью в штат некоторых организаций входит психолог.

Физические мероприятия примыкают к организационным. Они заключаются в применении человеческих ресурсов, специальных технических средств и устройств, обеспечивающих защиту от проникновения злоумышленников на объект, несанкционированного использования, порчи или уничтожения ими материальных и людских ресурсов. Такими человеческими ресурсами являются лица ведомственной или вневедомственной охраны и вахтеры, отдельные, назначаемые руководством организации, сотрудники.

В качестве технических средств используются решётки на окна, ограждения, металлические двери, турникеты, металодетекторы и др. Программно-технические средства включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения.

Для комплексного обеспечения безопасности объекты оборудуются системами связи, диспетчеризации, оповещения, контроля и управления доступом; охранными, пожарными, телевизионными и инженерными устройствами и системами; охранной, пожарной сигнализацией и автоматикой.

Успешному обеспечению безопасности способствуют заблаговременные мероприятия по выявлению и идентификации возможных угроз (опознание и предвидение, оценка, уменьшение вредного влияния их на человека и среду его обитания).

К инженерно-техническим средствам защиты относятся:

● специальное укрепление зданий и помещений;

● хранилища;

● системы пассивной безопасности (двери и металлоконструкции, замки, защитные стёкла, витрины и стенды, сейфы и металлические шкафы; преграждающие, ограждающие и запирающие устройства, ворота);

● средства индивидуальной защиты.

Эти же мероприятия способствуют защите программно-технических средств, людей и информации.

Защита работников и посетителей входит в состав общих организационных и технических мероприятий по защите организации от различных предвиденных и непредвиденных отрицательных воздействий.

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 – Firewalls, 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 персонал 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).

Литература:

1. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс] : учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург : Лань, 2022. - 344 с. - ISBN 978-5-8114-3940-9 : Б. ц.
2. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петурбург : Лань, 2022. - 324 с. - ISBN 978-5-8114-4067-2 : Б. ц.