УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией и законспектировать лекцию не меньше трех листов, составить и ответить на вопросы.

2. Предоставит отчет конспекта лекции прислать в виде скриншото в течении трех дней.

3. Отправить преподавателю на почту **v.vika2014@mail.ru** и указать свою Ф.И.О, группу, и название дисциплины тел 072-17-44-9-22

Тема: Защита информации от несанкционированного доступа.

Цель: ознакомиться с методами защиты от несанкционированного доступа.

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения компании.

Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Для грамотной защиты от несанкционированного доступа важно сделать следующее:

- отсортировать и разбить информацию на классы, определить уровни допуска к данным для пользователей;
- оценить возможности передачи информации между пользователями (установить связь сотрудников друг с другом).

В результате этих мероприятий появляется определенная иерархия информации в компании. Это дает возможность разграничения доступа к сведениям для сотрудников в зависимости от рода их деятельности.

Аудит доступа к данным должен входить в функционал средств информационной безопасности. Помимо этого, программы, которые компания решила использовать, должны включать следующие опции:

- аутентификация и идентификация при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток НСД;
- контроль работоспособности используемых систем защиты информации;

- обеспечение безопасности во время профилактических или ремонтных работ.

Идентификация и аутентификация пользователей

Для выполнения этих процедур необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя. Необходимо учитывать, что в ходе идентификации необязательно устанавливается личность. Возможно принятие любого другого идентификатора, установленного службой безопасности.

После этого следует аутентификация – пользователь вводит пароль или подтверждает доступ к системе с помощью биометрических показателей (сетчатка глаза, отпечаток пальца, форма кисти и т. п.). Кроме этого, используют аутентификацию с помощью USB-токенов или смарт-карт. Этот вариант слабее, так как нет полной гарантии сохранности или подлинности таких элементов.

Протоколы секретности для бумажной документации

Несмотря на повсеместную цифровизацию, традиционные бумажные документы по-прежнему используются в организациях. Они содержат массу информации – бухгалтерские сведения, маркетинговую информацию, финансовые показатели и прочие критические данные. Заполучив эти документы, злоумышленник может проанализировать масштабы деятельности организации, узнать о направлениях финансовых потоков.

Для защиты документации, содержащей сведения критической важности, используются специальные протоколы секретности. Хранение, перемещение и копирование таких файлов производится по специальным правилам, исключающим возможность контакта с посторонними лицами.

Защита данных на ПК

Для защиты информации, хранящейся на жестких дисках компьютеров, используются многоступенчатые средства шифрования и авторизации. При загрузке операционной системы используется сложный пароль, который невозможно подобрать обычными методами. Возможность входа в систему пользователя со стороны исключается путем шифрования данных в BIOS и использования паролей для входа в разделы диска.

Для особо важных устройств следует использовать модуль доверенной загрузки. Это аппаратный контроллер, который устанавливается на материнскую плату компьютера. Он работает только с доверенными пользователями и блокирует устройство при попытках включения в отсутствие владельца.

Также применяются криптографические методы шифрования данных, превращающие текст «вне системы» в ничего не значащий набор символов.

Эти мероприятия обеспечивают защиту сведений и позволяют сохранить их в неприкосновенности.

Определение уровней защиты

С методической точки зрения процесс защиты информации можно разделить на четыре этапа:

- предотвращение – профилактические меры, ограничение доступа посторонних лиц;
- обнаружение – комплекс действий, предпринимаемых для выявления злоупотреблений;
- ограничение – механизм снижения потерь, если предыдущие меры злоумышленникам удалось обойти;
- восстановление – реконструкция информационных массивов, которая производится по одобренной и проверенной методике.

Каждый этап требует использования собственных средств защиты информации, проведения специальных мероприятий. Необходимо учитывать, что приведенное разделение условно. Одни и те же действия могут быть отнесены к разным уровням.

Предотвращение сетевых атак

Компьютеры, подключенные к Интернету, постоянно подвергаются риску заражения вредоносным программным обеспечением. Существует масса ПО, предназначенного для отслеживания паролей, номеров банковских карт и прочих данных. Нередко вирусы содержатся в рассылках электронной почты, попадают в систему через сомнительные сетевые ресурсы или скачанные программы.

Для защиты системы от вредоносных программ, необходимо использовать антивирусные приложения, ограничить доступ в Сеть на определенные сайты. Если в организации параллельно используются локальные сети, следует устанавливать файрволы (межсетевые экраны).

Большинство пользователей хранит информацию в отдельных папках, которые названы «Пароли», «Мои карты» и т. п. Для злоумышленника такие названия являются подсказками. В названиях таких файлов необходимо использовать комбинации букв и цифр, ничего не говорящие посторонним людям. Также рекомендуется шифровать ценные данные в компьютерах и периодически производить их резервное копирование.

Какие результаты должны быть достигнуты

Грамотное использование систем защиты информации позволяет добиться благоприятных результатов:

- уменьшить риски утраты репутации и потери денежных средств;
- исключить потери научных разработок, интеллектуальной собственности, личных данных;
- снизить затраты на мероприятия по защите информации, исключению постороннего доступа к ценным сведениям.

Также служба ИБ должна настроить политики безопасности для всех подразделений и сотрудников, работающих с конфиденциальной информацией разного типа:

- финансовая документация;
- клиентские базы данных;
- научные и технологические разработки, другая интеллектуальная собственность;
- сведения, составляющие банковскую тайну;
- персональная информация сотрудников или иных лиц.

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

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.

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 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.

Программно-техническая и физическая защита от несанкционированных воздействий

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., арочные металодетекторы). 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 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. Пример современного считывающего отпечатки пальцев устройства представлен на рис. 5.6.

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.

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.