УДК 681.322.067

С.В. Корякин
Институт автоматики и информационных технологий
Национальной академии наук Кыргызской Республики, г.Бишкек
s.koryakin@aknet.kg

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются особенности построения и функционирования систем информационной безопасности, комплекс организационных и технических мер, направленных на защиту корпоративных данных. Обосновываются процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты и т. д. Рекомендуются технические меры в использовании аппаратных и программных средств контроля доступа, мониторинга утечек, антивирусной защиты, межсетевого экранирования, защиты от электромагнитных излучений и прочее.

Ключевые слова: информационная безопасность, системы, информация, данные, средства защиты, устройства, технические средства, технические меры.

В наше время при бурном развитии науки и техники большое внимание необходимо уделять инженерно-технической охране объектов. Мероприятия по организации охраны являются частью единой системы охраны секретной информации объекта.

В решении вопросов обеспечения охраны объекта и территории участвуют определенные силы и средства, от эффективного функционирования которых зависит своевременное предотвращение доступа лиц к информации (материальным ценностям), которые охраняются посредством пропускного/внутри объектового режимов. Их целью является предупреждение любых происшествий на объекте, а также попыток проникновения на его территорию посторонних (в частности, ликвидация последствий происшествий), своевременное обнаружение проникших на территорию злоумышленников и их задержание, обеспечение сохранности, как конфиденциальной информации, так и материальных средств.

Список инженерно-технических средств защиты объектов

Список инженерно-технических средств защиты объектов можно разделить на физические барьеры и непосредственно технические средства.

Физические барьеры создаются исходя из степени секретности деятельности предприятия и расположения его объектов. К ним относят [1]:
Спец конструкции (контейнеры и решетки, усиленные двери, различные противотаранные устройства и пр.); строительные конструкции на объектах (ворота и двери, перекрытия и пр.); иные препятствия. Технические средства размещают по периметру, как служебных помещений, так и всех зон и элементов объектов.

К основным техническим средствам относят:

- средства охранной сигнализации – устанавливают на КПП, в служебных помещениях, во всех зданиях/сооружениях охраняемой зоны объекта;
- средства спец/связи (включая экстренную);
- средства контроля доступа – устанавливают на КПП, в служебных помещениях, во всех зданиях/сооружениях охраняемой зоны объекта; средства систем жизнеобеспечения и обнаружения (при попытке проноса/провоза) запрещенных веществ, предметов; средства наблюдения.

Особое место в единой системе защиты занимают различные средства наблюдения, охранная сигнализация и, конечно, средства контроля доступа. Все технические средства системы защиты обеспечены автоматической системой переключения на резервный источник питания в случае отключения основного.

Технические системы противопожарной защиты объектов:

Средства эвакуации (речевые оповещатели, пути эвакуации и пр.); системы контроля доступа, видеонаблюдения + охранная сигнализация; грамотный выбор и размещение дымовых извещателей с компенсацией запыленности. Идеальный вариант – комбинированные или совмещенные устройства для снижения числа ложных срабатываний, для обнаружения лица при температуре выше температуры тела.

Использование ИК-извещателей с микропроцессорной обработкой.

Организационные меры – плановые обходы территории, создание регламента для охранников и контроль над следованием ему, четко продуманная система пропуска, мониторинг камер наблюдения и зональная сигнализация, подключение коммуникаторов для вывода всей информации на пульты МЧС и ЧВК, и пр.

Дополнительные меры организации. Они касаются не только здания, но и всей территории, прилегающей к предприятию, включая парковки. Например, решение проблемы подъезда в экстренных случаях пожарных автомобилей, то есть, для эффективного решения задач необходимо соединение всех элементов системы безопасности в единую систему.

Выбор и размещение датчиков (пламени, тепловых, дымовых).

Следующими в списке средств защиты стоят виды технической защиты объектов от незаконного проникновения – сигнализация и видеонаблюдение.

При охране предприятия используются следующие виды сигнализации: охранная, пожарная, тревожная.

Очень распространен способ, когда первые две системы объединяют в одну. Назначение данной охранно-пожарной сигнализации – сигнализирование о пожаре либо попытке противоправного проникновения на территорию.

Назначение тревожной сигнализации – сигнализирование о разбойном нападении и прочих действиях незаконного характера, осуществляемое посредством нажатия тревожных кнопок (скрыто установленных) персоналом.

Сигнализацию разделяют на: автономную – выдача у доверенных лиц различных звуковых/световых сигналов тревоги и централизованная – выдача сигналов тревоги на приборах охраны, КПП или дежурной части милиции.

Различают следующие элементы технической укрепленности объектов:

Средства связи. Средства наблюдения. Освещение объекта охраны. Запретная зона. Ограждение периметра. Запорные устройства. Нахождение сотрудников охраны на спец местах (постовые будки, спец вышки, места скрытого наблюдения и пр.). Основные исходные требования к технической оснащенности объектов: исправное состояние всех помещений и их элементов; соответствие дверей требованиям ГОСТа.

Остекленные окна (форточки и пр.) с наличием исправных запорных систем, решеток при необходимости и пр. Установка решетчатых дверей при отсутствии дверей в подвальные помещения. Установка решеток на вентиляционные шахты либо дымоходы с выходом на крышу. Применение специальных запорных устройств. Тех оснащение спец хранилищ. Оборудование помещений с ценностями группы А различными замками повышенной секретности и многоуровневыми тех средствами, автономным источником питания и сигнализацией. Снабжение поста охраны внешней/внутренней связью. Укомплектование объекта нужным количеством средств пожаротушения и всеми видами сигнализации. Обеспечение достаточного освещения на территории объекта и прилегающей к нему.

Организация технической защиты помещений

Ключевая задача инженерно-технической защиты – предупреждение проникновения случайных лиц и злоумышленников на территорию объекта. Данная система защиты разделяется на 6 специальных зон: Помещения, которые доступны посетителям. Периметр объекта. Периметр прилегающей территории. Кабинеты руководства. Служебные помещения. Сеймовые комнаты, хранилища и пр.

Основные средства инженерно-технической защиты:

Заборные ворота и заборы (ток высокого напряжения, колючая проволока, козырьки и пр.). Шлюзы (пропуск/проверка авто). КПП для пропуска посетителей, персонала. Укрепление дверей, решеток, окон. Специальные электрические замки. Тамбуры, оснащенные средствами безопасности, и пр.

Таким образом, в настоящее время в современном обществе информационная сфера имеет две составляющие [2]: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Определение и классификация возможных угроз безопасности

Также важным аспектом информационной безопасности является определение и классификация возможных угроз безопасности.

Информационная безопасность в следующих значениях может рассматриваться как процесс обеспечения конфиденциальности, целостности и доступности информации (рис 1) [3].

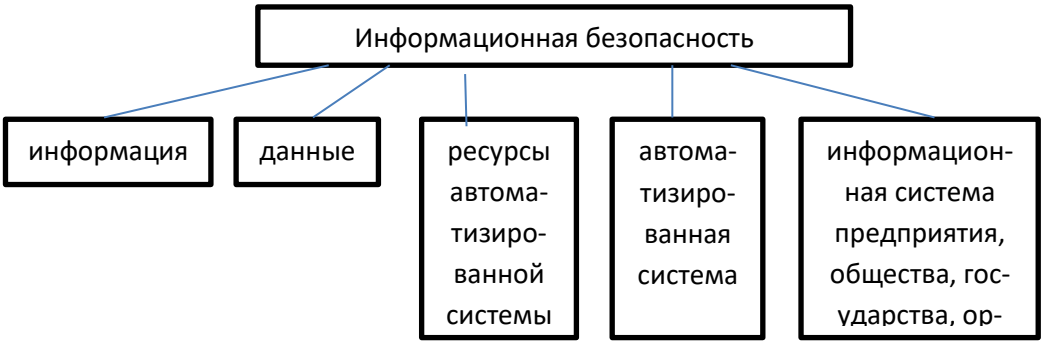

Рисунок. 1. Значение состояния определенного объекта системы информационной безопасности

Рассмотрим структурную схему основных критериев в совокупности составляющих систему информационной безопасности (рис. 2).

Безопасность автоматизированной информационной системы [4] характеризует состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов. Защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений. Поддерживающая инфраструктура – системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал.

В современном обществе информационную безопасность определяют, как "процесс баланса между возникающими, воздействующими угрозами и успешностью противодействия этим угрозам со стороны органов государственной власти, отвечающих за безопасность государства" [5].

Рисунок. 2. Структурная схема критериев системы информационной безопасности

В качестве стандартной модели безопасности часто приводят модель из трёх категорий (табл. 1):

Таблица 1. Категории моделей информационной безопасности

Конфиденциальность	Целостность	Доступность
Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право	Избежание несанкционированной модификации информации	Избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа

Существуют и другие не всегда обязательные категории модели безопасности (табл. 2):

Таблица 2. Не обязательные категории модели информационной безопасности

Неотказуемость или апеллируемость	Подотчётность	Достоверность	Аутентичность или подлинность
способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты	свойство, обеспечивающее однозначное прослеживание действий любого логического объекта	свойство соответствия предусмотренному поведению или результату	свойство, гарантирующее, что субъект или ресурс идентичны заявленным

Определение категорий и характеристик информационной безопасности наиболее удобно проводить при помощи системного подхода. Системный подход при описании информационной безопасности предлагает выделить следующие составляющие [6]: Законодательная, нормативно-правовая и научная база. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ. Организационно-технические и режимные меры и методы (Политика информационной безопасности). Программно-технические способы и средства обеспечения информационной безопасности.

Для построения и эффективной эксплуатации систем обеспечения информационной безопасности (СОИБ) необходимо [7]: выявить требования защиты информации, специфические для данного объекта защиты; учесть требования национального и международного законодательства; использовать наработанные практики (стандарты, ме-

тодологии) построения подобных СОИБ; определить подразделения, ответственные за реализацию и поддержку СОИБ; распределить между подразделениями области ответственности в осуществлении требований СОИБ; на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты; реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации; реализовать систему менеджмента (управления) информационной безопасности (СМИБ); используя СМИБ, организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.

На (рис. 3) изображены службы, организующие защиту информации.

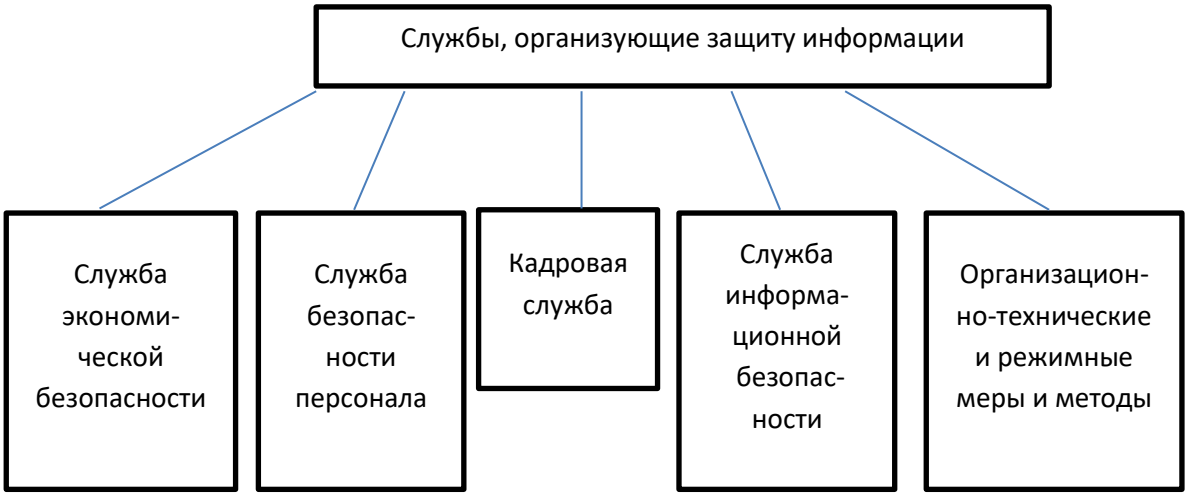

Рисунок. 3. Службы, организующие защиту информации

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая Политика информационной безопасности или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) (англ. Organizational security policy) [8] – совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. Правила, директивы, сложившаяся практика, которые определяют, как в пределах структуры и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию. Структурная схема основных критериев построения Политики информационной безопасности изображена на Рис. 4.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы [9]: защита объектов информационной системы; защита процессов, процедур и программ обработки информации; защита каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.), включая защиту информации в локальных сетях;
подавление побочных электромагнитных излучений; управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

- определение информационных и технических ресурсов, подлежащих защите;
- Выявление полного множества потенциально возможных угроз и каналов утечки информации;

- проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- определение требований к системе защиты;
- осуществление выбора средств защиты информации и их характеристик;
- Внедрение и организация использования выбранных мер, способов и средств защиты;
- Осуществление контроля целостности и управление системой защиты.

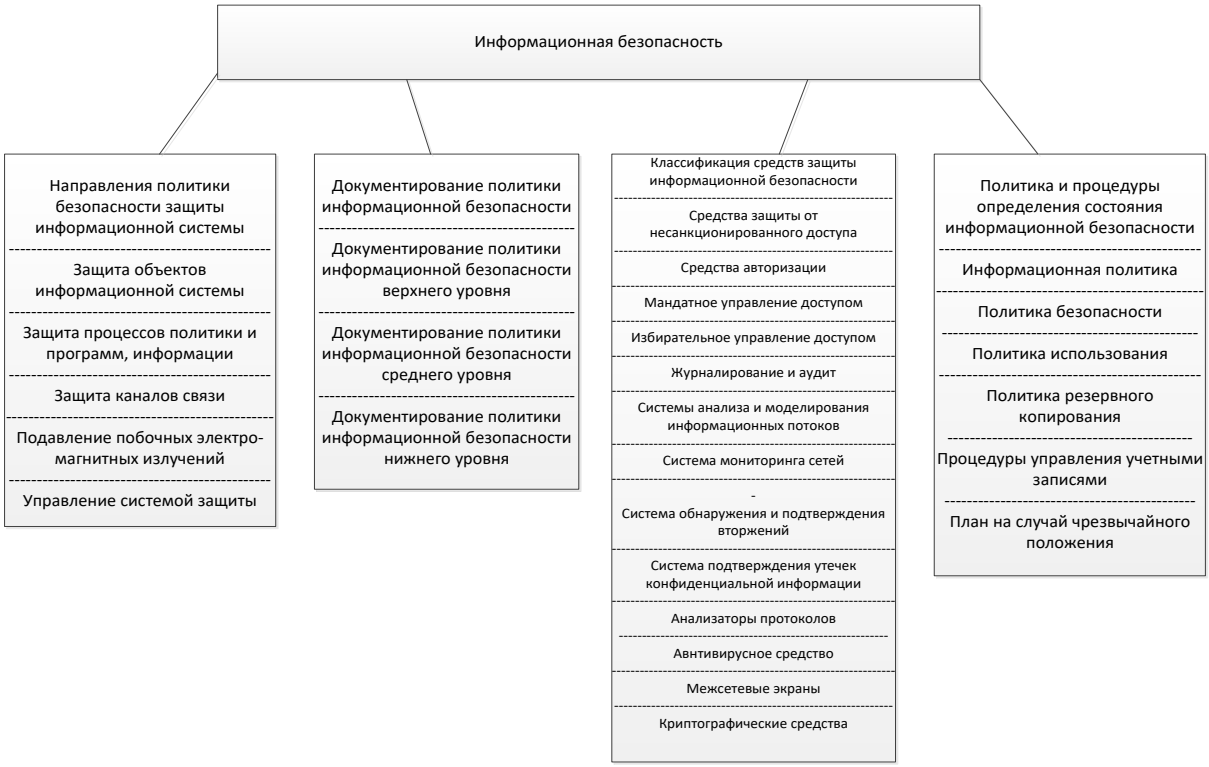

Рисунок. 4. Структурная схема критериев построения

Политика информационной безопасности

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты – верхний уровень, средний уровень, нижний уровень.

Документы верхнего уровня Политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. Подобные документы могут называться «Концепция ИБ», «Регламент управления ИБ», «Политика ИБ», «Технический стандарт ИБ» и т. п. Область распространения документов верхнего уровня обычно не ограничивается, однако данные документы могу т выпускаться и в двух редакциях – для внешнего и внутреннего использования.

Согласно ГОСТ Р ИСО/МЭК 17799-2005, на верхнем уровне Политики информационной безопасности должны быть оформлены следующие документы: «Концепция обеспечения ИБ», «Правила допустимого использования ресурсов информационной системы», «План обеспечения непрерывности бизнеса».

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты

информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации. Например: Безопасности данных, Безопасности коммуникаций, использования средств криптографической защиты, Контентная фильтрация и т. п. Подобные документы обычно издаются в виде внутренних технических и организационных политик (стандартов) организации. Все документы среднего уровня политики информационной безопасности конфиденциальны.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Далее в списке средств защиты располагаются Программно-технические способы и средства обеспечения информационной безопасности. Определяют следующую классификацию способов и средств защиты информации [10]:

- средства защиты от несанкционированного доступа;
- средства авторизации;
- мандатное управление доступом [11];
- избирательное управление доступом;
- управление доступом на основе ролей;
- журналирование (так же называется Аудит);
- системы анализа и моделирования информационных потоков (CASE-системы); системы мониторинга сетей; системы обнаружения и предотвращения вторжений (IDS/IPS);
- системы предотвращения утечек конфиденциальной информации (DLP-системы);
- анализаторы протоколов; антивирусные средства; межсетевые экраны.

Криптографические средства – шифрование; цифровая подпись; системы резервного копирования; системы бесперебойного питания; источники бесперебойного питания; резервирование нагрузки; генераторы напряжения.

Системы аутентификации: пароль; ключ доступа (физический или электронный); сертификат; биометрия.

Средства предотвращения взлома корпусов и краж оборудования. Средства контроля доступа в помещения.

Инструментальные средства анализа систем защиты – антивирус, способы защиты от компьютерных злоумышленников

Исходя из этой классификации средств защиты информации, понятие информационная безопасность это, прежде всего, защита сети от различного вида атак. Существует ряд простых средств, с помощью которых можно остановить попытки проникновения в сеть. К ним относятся:

Оперативная установка исправлений для программ, работающих в интернете.

Антивирусные программы по обнаружению различного рода взломов и вирусов незаменимы для повышения безопасности любой сети. Они наблюдают за работой компьютеров и выявляют на них вредоносные программы.

Следует использовать наиболее надёжные пароли, менять их как можно чаще и чтобы их длина была максимальной. Это может предотвратить кражу секретной и не секретной информации.

Соединения с удаленными машинами (компьютерами) должны быть защищены с помощью паролей, чтобы избежать проникновения в сеть с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей.

При установке новой операционной системы обычно разрешаются все сетевые средства, что является не безопасным. Кроме вышеперечисленных средств защиты информации, существует еще множество способов предотвращения взломов и краж информации. Для избегания неприятных ситуаций необходимо изучать рекомендации по безопасности и придерживаться необходимых средств защиты.

Следующей в списке средств защиты располагается – Организационная защита объектов информатизации.

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает: организацию охраны, режима, работу с кадрами, с документами, использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности [12].

К основным организационным мероприятиям относятся:
организацию режима и охраны. Их цель – исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.; организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учёт, исполнение, возврат, хранение и уничтожение; организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению её защиты; организацию работы по проведению систематического контроля над работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях: обеспечение защищённого хранения информации на носителях; защита данных, передаваемых по каналам связи; создание резервных копий, послеаварийное восстановление и т. д.

Обеспечение информационной безопасности – это непрерывный процесс, включающий в себя пять ключевых этапов: оценка стоимости, разработка политики безопасности, реализация политики, квалифицированная подготовка специалистов, аудит.

Основные виды оценки: Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.

Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры, выявлены зоны риска.

Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов.

Аудит. Исследованы существующая политика и соответствие организации этой политике.

Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение.

При проведении оценки должны быть исследованы такие документы, как: политика безопасности; информационная политика; политика и процедуры резервного копирования; справочное руководство работника или инструкции; процедуры наймаувольнения работников; методология разработки программного обеспечения; методология смены программного обеспечения; телекоммуникационные политики; диаграммы сети.

Получив вышеуказанные политики и процедуры, каждую из них исследуют на предмет значимости, правомерности, завершенности и актуальности, так как политики и процедуры должны соответствовать цели, определенной в документе.

После оценки необходимо заняться разработкой политик и процедур, которые определяют предполагаемое состояние безопасности и перечень необходимых работ. Нет политики – нет плана, на основании которого организация разработает и выполнит эффективную программу ИБП.

Необходимо разработать следующие политики и процедуры:

Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.

Политика безопасности. Определяет технические средства управления для различных компьютерных систем.

Политика использования. Обеспечивает политику компании по использованию компьютерных систем.

Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.

Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.

План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Последний шаг в процессе реализации информационной безопасности Аудит. Он определяет состояние информационной безопасности внутри организации, создание соответствующих политик и процедур, приведение в действие технических средств контроля и обучение персонала [13].

Обеспечение системы информационной безопасности возможно только при системном и комплексном подходе к защите. Полноценная политика информационной безопасности подразумевает непрерывный контроль всех важных событий и состояний, влияющих на безопасность данных, и осуществляется круглогодично.

Информационная безопасность системы достигается целым комплексом организационных и технических мер, направленных на защиту корпоративных данных. Организационные меры включают документированные процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты и т. д. Технические меры заключаются в использовании аппаратных и программных средств контроля доступа,

мониторинга утечек, антивирусной защиты, межсетевого экранирования, защиты от электромагнитных излучений и прочее.

Подводя итог, хочу отметить что, в современном обществе для обеспечения максимальной защиты информации необходимо создавать системы информационной безопасности с временными ограничениями, которые в автоматизированном режиме производят выработку управляющих воздействий и команд, поступающий на реальный объект управления. Что позволит осуществлять защиту информационных ресурсов в нужное время в нужном месте, то есть здесь и сейчас.

Литература

1. *Симонов С.* Современные технологии анализа рисков в информационных системах // PCWEEK. – 2001. – № 37.
2. *Грушо А. А., Тимонина, Е.Е.* Ценность информации // Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996. – С. 52–55.
3. *Бармен Скотт*. Разработка правил информационной безопасности. М.: Вильямс, 2002. – 208 с.
4. *Галатенко В. А.* Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006. – 264 с.
5. *Галицкий А. В., Рябко С. Д., Шаньгин В. Ф.* Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. – 616 с.
6. *Лепехин А. Н.* Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. – 176 с.
7. *Запечнико С. В., Милославская Н. Г., Толстой А. И., Ушаков Д.В.* Информационная безопасность открытых систем. Том 1. – М.: Горячая линия – Телеком, 2006. Том 2. – М.: Горячая линия – Телеком, 2008. – 560 с.
8. *Лопатин В. Н.* Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. – 428 с.
9. *Родичев Ю.* Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. – 272 с.
10. *Петренко С. А., Курбатов, В. А.* Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.
11. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. – 544 с.
12. *Малюк А. А.* Теория защиты информации. – М.: Горячая линия – Телеком, 2012. – 184 с.
13. *Щербако А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.