ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 63 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 63 кафедры
полковник_____С.Войцеховский

«___» _____ 2015 г.

Автор: преподаватель 63 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 19

Тема: «КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 63 кафедры
протокол № __ «____» _____ 2015 г.

Санкт-Петербург
2015

Содержание занятия и время

Введение……13-15 мин.

Учебные вопросы (основная часть):

1. Принципы построения комплексной системы информационной безопасности объекта. – 20 мин.

2. Порядок разработки комплексной системы обеспечения информационной безопасности объекта. – 10 мин.

3. Основные этапы создания системы информационной безопасности – 10 мин.

4. План мероприятий по защите служебной или коммерческой тайны. – 10 мин.

5. Организационные меры обеспечения защиты информации. – 10 мин.

6. Автоматизированный комплекс обеспечения безопасности – 10 мин.

Заключение……....5-7 мин.

Литература:

1. план-конспект.
2. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
3. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.
4. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000.- 450 с.
6. Общесистемные вопросы защиты информации. Коллективная монография/ под ред. Е.М. Сухорева. Кн. 1 – М.: Радиотехника, 2003. – 296 с.
7. Основы современных компьютерных технологий: Учебник/ под ред. Проф. А.Д.Хомоненко – СПб.: КОРОНА принт, 2005. – 672 с.
8. Петренко С.А., Петренко А.А. Аудит безопасности INTRANET. – М.: ДМК Пресс, 2002. – 416 с.
9. Соколов А.В., Шаньгин В.Ф. Защита информации в распределённых корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

Материально-техническое обеспечение:

1. Наглядные средства обучения - доска, мел.

Организационно-методические указания:

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом в течение 10 мин. произвести опрос курсантов по пройденному материалу в виде летучки № 3.

Метод проведения занятия – рассказ. В основной части сконцентрировать внимание курсантов на важности комплексного подхода к защите информации и основных этапах создания системы информационной безопасности.

За 3 – 5 мин. до конца занятия делаю обобщающие выводы, задаю контрольные вопросы для проверки, как военнослужащие усвоили тему занятия:

1. Перечислите основные требования, предъявляемые к комплексной системе защиты информации.
2. Перечислите последовательность действий при разработке комплексной системы обеспечения информационной безопасности объекта.
3. Перечислите основные мероприятия, которые можно отнести к «разовым мероприятиям» построения КСИБ.
4. Перечислите основные мероприятия, которые можно отнести к «периодически проводимым мероприятиям» построения КСИБ.
5. Перечислите основные мероприятия, которые можно отнести к «мероприятиям, проводимым по необходимости» для построения КСИБ.
6. Перечислите основные мероприятия, которые можно отнести к «постоянно проводимым мероприятиям» для построения КСИБ.

Отвечаю на вопросы по теме занятия, даю задание на самоподготовку.

Лекция № 19

Принципы построения комплексной системы информационной безопасности объекта

Анализ состояния дел в области информационной безопасности показывает, что в ведущих странах сложилась **достаточно четко очерченная система концептуальных взглядов на проблемы информационной безопасности.**

И, тем не менее, как свидетельствует реальность, злоумышленные действия над информацией не только не уменьшаются, а имеют достаточно устойчивую тенденцию к росту.

Это свидетельствует о том, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация обеспечения безопасности информационной системы.

Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов.

Первым и наиболее важным является принцип непрерывности совершенствования и развития системы информационной безопасности. Суть этого принципа заключается в постоянном контроле функционирования системы, выявлении ее слабых мест, потенциально возможных каналов утечки информации и НСД, обновлении и дополнении механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты информации. Таким образом, обеспечение информационной безопасности не может быть одноразовым актом.

Вторым является принцип комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации.

Комплексный характер защиты информации проистекает, прежде всего, из характера действий злоумышленников, стремящихся любой совокупностью средств добыть важную для конкурентной борьбы информацию. Здесь правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения.

Кроме того, наибольший эффект достигается в том случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм — систему информационной безопасности. Только в этом случае появляются системные свойства не

присущие ни одному из отдельных элементов системы защиты, а также возможность управлять системой, перераспределять ее ресурсы и применять современные методы повышения эффективности ее функционирования.

Можно определить систему информационной безопасности как организованную совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа к ней.

Важнейшими условиями обеспечения безопасности являются *законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм* представителей службы информационной безопасности, *подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.*

Без соблюдения этих условий никакая система информационной безопасности не может обеспечить требуемого уровня защиты.

С позиций системного подхода для реализации приведенных принципов процесс, да и сама комплексная система защиты информации должны отвечать некоторой совокупности требований.

Комплексная система защиты информации должна быть:

- централизованной; необходимо иметь в виду, что процесс управления *всегда централизован*, в то время как *структура системы*, реализующей этот процесс, должна *соответствовать структуре защищаемого объекта*;
- плановой; планирование осуществляется для организации взаимодействия всех подразделений объекта в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;
- конкретной и целенаправленной; защите подлежат абсолютно конкретные информационной ресурсы, могущие представлять интерес для конкурентов;
- активной; защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом “обнаружить и устранить” принцип “предвидеть и предотвратить”;
- надежной и универсальной, охватывать весь технологический комплекс информационной деятельности объекта; методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;
- нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;
- открытой для изменения и дополнения мер обеспечения безопасности информации;
- экономически эффективной; затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями существует ряд устоявшихся рекомендаций, которые будут не бесполезны создателям систем информационной безопасности:

- средства защиты должны быть просты для технического обслуживания и “прозрачны” для пользователей;
- каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;
- возможность отключения защиты в особых случаях, например, когда механизмы защиты реально мешают выполнению работ;
- независимость системы защиты от субъектов защиты;

- разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты;
- отсутствие на предприятии излишней информации о существовании механизмов защиты.

Все перечисленные позиции должны лечь в основу формирования системы защиты информации.

При обеспечении информационной безопасности существует два аспекта:

- формальный, связанный с определением критериев, которым должны соответствовать защищаемые информационные технологии;
- практический, характеризующий порядок определения конкретного комплекса мер безопасности применительно к рассматриваемой информационной технологии.

Критерии, которым должны соответствовать защищаемые информационные технологии, являются объектом стандартизации более пятнадцати лет. В настоящее время разработан проект международного стандарта “Общие критерии оценки безопасности информационных технологий”. Несмотря на существенную разницу в методологии обеспечения базового и повышенного уровней безопасности, можно говорить о единой концепции ИБ.

Изложенные основные концептуальные положения являются основой механизма выработки детальных предложений по формированию политики и построению комплексной системы информационной безопасности.

Последовательность действий при разработке комплексной системы обеспечения информационной безопасности объекта

Прежде, чем приступать к разработке комплексной системы информационной безопасности, необходимо определить, что же для организации (физического лица) является интеллектуальной собственностью.

С точки зрения делового человека, интеллектуальной собственностью являются информационные ресурсы, знания, которые помогают ему эффективно разрабатывать и изготавливать новую продукцию, выгодно продавать товар или каким-то другим образом увеличивать свою прибыль. Способ управления производством, технологический процесс, список клиентов профиль научных исследований, анализ конкурентоспособности – лишь некоторые примеры тому.

Незнание того, что составляет интеллектуальную собственность — уже шаг к потерям финансовым, моральным и материальным. Именно с этого надо начинать создание системы защиты информации.

Дальнейшими этапами, вне зависимости от размеров организации и специфики ее информационной системы, в том или ином виде должны быть:

- определение границ управления информационной безопасностью объекта;
- анализ уязвимости;
- выбор контрмер, обеспечивающих информационную безопасность; определение политики информационной безопасности;
- проверка системы защиты;
- составление плана защиты;
- реализация плана защиты (управление системой защиты).

Любые действия по созданию системы информационной безопасности должны заканчиваться определенными результатами в виде документа или технического решения (см. рис. 1).

Как показывает разработка реальных систем, ни один из способов (мер, средств и мероприятий) обеспечения безопасности информации не является надежным, а максимальный эффект достигается при объединении всех их в целостную систему защиты информации. Только оптимальное сочетание организационных, технических и программных мероприятий, а также постоянное внимание и контроль над поддержанием системы защиты в актуальном состоянии позволит с наибольшей эффективностью обеспечить решение постоянной задачи.

Методологические основы обеспечения информационной безопасности являются достаточно общими рекомендациями, базирующимися на мировом опыте создания подобных систем. Задача каждого специалиста по защите информации преломить абстрактные положения к своей конкретной предметной области (предприятию, организации, банка), в которых всегда найдутся свои особенности и тонкости этого не простого ремесла.

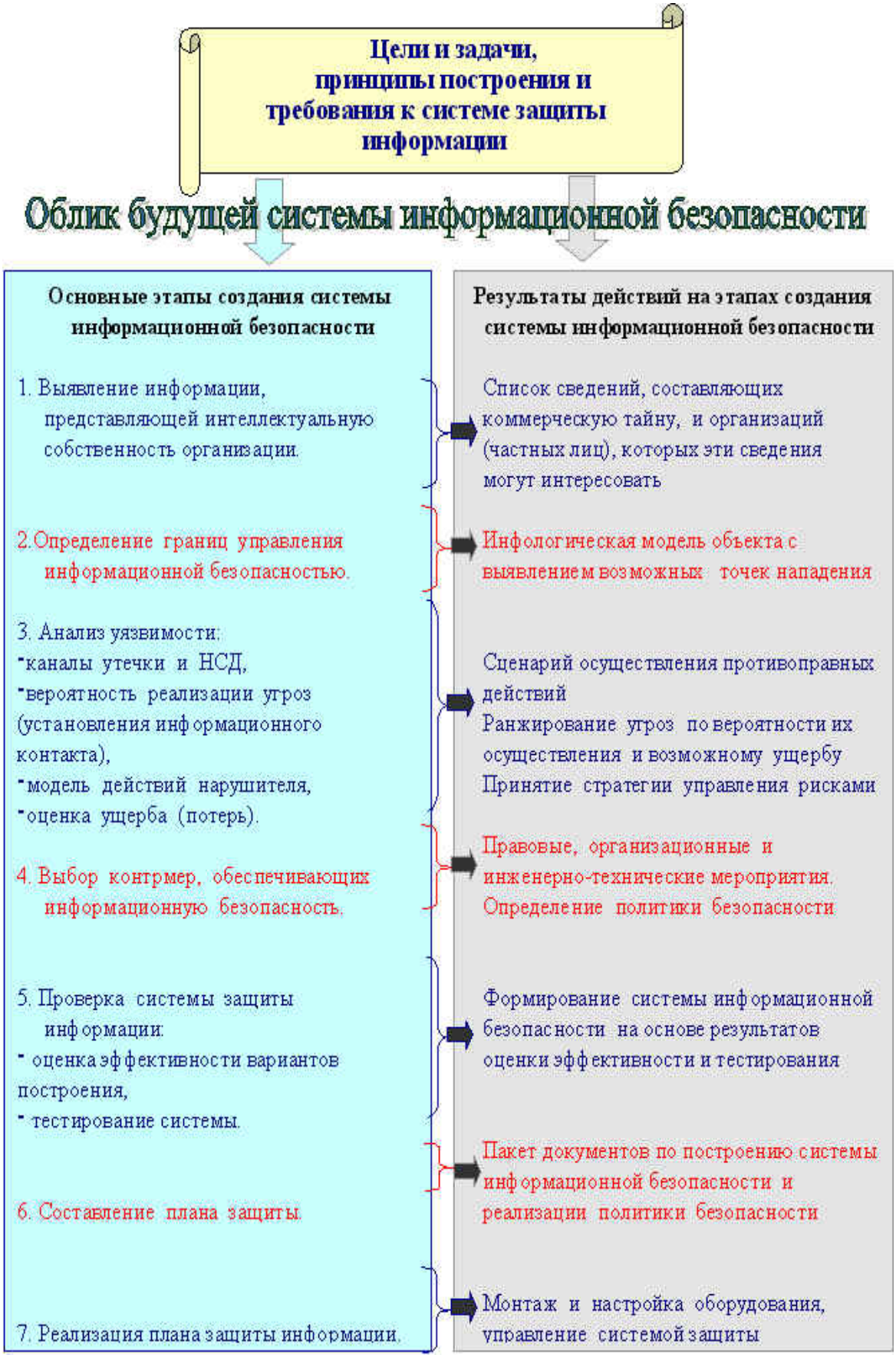

Рис. 1

ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ СЛУЖЕБНОЙ ИЛИ КОММЕРЧЕСКОЙ ТАЙНЫ ОРГАНИЗАЦИИ НА 200_ г.

(вариант)

1. Цели плана по защите служебной или коммерческой тайны.

Ими могут быть:

- предотвращение несанкционированного распространения служебных, коммерческих или конфиденциальных секретов;
- предотвращение разглашения служебных или коммерческих секретов сотрудниками и другими носителями таких секретов, а также исключение утечки по техническим каналам.

2. Анализ сведений, составляющих служебную или коммерческую тайну:

- определить, какие сведения организации могут быть отнесены к служебной или коммерческой тайне;
- установить места их разработки, накопления и хранения;
- выявить потенциальные каналы утечки таких сведений;
- оценить возможности по перекрытию этих каналов;
- проанализировать соотношение затрат и доходов по использованию различных технологий, обеспечивающих защиту служебной или коммерческой тайны;
- назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы безопасности по следующим направлениям:

- контроль сооружений и оборудования организации, обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений организации и т. д.;
- разработка памятки о сохранении служебной или коммерческой тайны, определение порядка ознакомления с ней, а также с Перечнем сведений, составляющих такие тайны;
- работа с персоналом организации, в том числе проведение бесед при приеме на работу, инструктаж вновь принятых на работу по правилам и процедурам защиты служебной или коммерческой тайны
- в организации, получение от них обязательств (контрактов) о неразглашении, обучение сотрудников правилам сохранения служебных и коммерческих секретов, стимулирование соблюдения конфиденциальности, беседы с увольняющимися и получение от них подписок;
- организация работы с конфиденциальными документами, установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами и их публикациями, контроль и учет технических носителей конфиденциальных сведений, засекречивание, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов;
- работа с конфиденциальной информацией, циркулирующей в технических средствах и системах обеспечения производственной и трудовой деятельности (создание системы защиты технических каналов защиты утечки информации);
- работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за работой пользователей на ПЭВМ);
- защита служебной или коммерческой тайны в организационно-правовых вопросах и особенно в процессе заключения контрактов и договоров с коллективом, сотрудниками, смежниками, поставщиками и т. д.

Организационные меры обеспечения защиты информации

С чего начинается информационная безопасность компьютерных сетей предприятия? Теория говорит об анализе рисков, выработке политики и организации системы безопасности. И это правильно. Но прежде чем обратиться к теории, надо навести элементарный порядок и наладить дисциплину в информационных службах предприятия.

Вы должны уметь четко ответить на вопросы:

- Сколько компьютеров (коммуникационного, вспомогательного оборудования) установлено на вашем предприятии? Сколько их сейчас, в данный момент, а не сколько их было вчера или месяц назад; сколько их на рабочих местах, сколько в ремонте, сколько в резерве.
- Вы сумеете узнать каждый компьютер "в лицо"?
- Обнаружите ли вы "маскарад" оборудования, когда какой-нибудь компьютер или его часть, или программное обеспечение подменены, так что кажущееся рабочей лошадкой оборудование на самом деле является троянским конем?
- Какие задачи и с какой целью решаются на каждом компьютере?
- Уверены ли вы в необходимости каждой единицы контролируемого вами оборудования и в том, что среди него нет ничего лишнего, установленного, скажем, для красоты и ждущего, чтобы на него обратил внимание какой-нибудь хакер из числа молодых и дерзких сотрудников? Ведь если от оборудования нет пользы, с точки зрения информационной безопасности от него можно ожидать только вреда.
- Каков порядок ремонта и технической профилактики компьютеров?
- Как проверяется оборудование, возвращаемое из ремонта, перед установкой на штатное рабочее место?
- Как производится изъятие и передача компьютеров в подразделения и каков порядок приема в работу нового оборудования?

Список вопросов можно продолжить... Аналогичные вопросы можно задать и относительно программного обеспечения и персонала.

Другими словами, защита информации начинается с постановки и решения организационных вопросов. Те, кому уже приходилось на практике заниматься вопросами обеспечения информационной безопасности в автоматизированных системах, единодушно отмечают следующую особенность - реальный интерес к проблеме защиты информации, проявляемый менеджерами верхнего уровня, на уровне подразделений, отвечающих за работоспособность автоматизированной системы организации сменяется на резкое неприятие.

Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

- появление дополнительных ограничений для конечных пользователей и специалистов подразделений обеспечения, затрудняющие использование и эксплуатацию автоматизированной системы организации;
- необходимость дополнительных материальных затрат как на проведение таких работ, так и на расширение штата специалистов, занимающихся проблемой информационной безопасности.
- экономия на информационной безопасности может выражаться в различных формах, крайними из которых являются:
- принятие только организационных мер обеспечения безопасности информации в корпоративной сети (КС);
- использование только дополнительных технических средств защиты информации (ТСЗИ).

В первом случае, как правило, разрабатываются многочисленные инструкции, приказы и положения, призванные в критическую минуту переложить ответственность с людей, издающих эти документы на конкретных исполнителей. Естественно, что требования таких документов (при отсутствии соответствующей технической поддержки) затрудняют повседневную деятельность сотрудников организации и, как правило, не выполняются.

Во втором случае, приобретаются и устанавливаются дополнительные ТСЗИ. Применение ТСЗИ без соответствующей организационной поддержки также неэффективно в связи с тем, что без установленных правил обработки информации в КС применение любых ТСЗИ только усиливает существующий беспорядок. Рассмотрим комплекс организационных мер, необходимых для реализации защиты информации в сетях ЭВМ. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Организационные меры:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой КС или внешней среде (по необходимости);
- периодически проводимые (через определенное время) мероприятия;
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия:

- общесистемные мероприятия по созданию научно-технических и методологических основ (концепции и других руководящих документов) защиты КС;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т. п.);
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т. п.);
- проведение спецпроверок всех применяемых в КС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;
- разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т. п.) по вопросам обеспечения безопасности программно-информационных ресурсов КС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитражем, третейским

судом) о правилах разрешения споров, связанных с применением электронной подписи;

- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- мероприятия по созданию системы защиты КС и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием КС, а также используемых при их решении режимов обработки и доступа к данным; определение перечня файлов и баз данных содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в КС; выявление наиболее вероятных угроз для данной КС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней; оценку возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);
- организацию надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т. п.;
- организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);
- создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации;
- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т. п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы,
- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;
- периодически с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;
- мероприятия по пересмотру состава и построения системы защиты.

Мероприятия, проводимые по необходимости

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т. п.);
- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.).

Постоянно проводимые мероприятия:

- мероприятия по обеспечению достаточного уровня физической защиты всех компонентов КС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т. п.).
- мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;
- явный и скрытый контроль за работой персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС;
- постоянно (силами отдела (службы) безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

Несколько детализируя методологию построения систем информационной безопасности относительно корпоративной сети, а также учитывая вышесказанное по возможным угрозам сети и имеющимся способам борьбы с ними, алгоритм построения системы информационной безопасности корпоративной сети может быть представлен следующим образом.

Весь объект защиты имеет несколько направлений возможных атак. Для каждого вида атаки существуют соответствующие способы и средства борьбы с ними. Определив основные способы борьбы, мы тем самым сформируем политику информационной безопасности. Выбрав в соответствии со сформированной политикой совокупность средств обеспечения информационной безопасности, объединив их системой управления, мы получим фактически систему защиты информации.

Аналогичным образом анализируются угрозы на уровне корпоративной сети. Она может быть представлена тремя основными составляющими – техническое обеспечение, информационное обеспечение и программное обеспечение. Каждый из этих компонент может далее детализироваться до степени, достаточной для формулировки основных угроз на этом уровне и возможных способов борьбы с ними.

Выбор конкретных способов и средств защиты информации на уровне сети также выливается в соответствующую политику и систему информационной безопасности, которые органически вливаются в общую политику и систему информационной безопасности всего объекта (**см. ниже схемы “Вероятные угрозы”**).


Вероятные угрозы всему информационному объекту
Возможные меры борьбы с угрозами
Политика информационной безопасности
Средства реализации мер борьбы с угрозами
Система информационной безопасности


Вероятные угрозы всему информационному объекту
Проникновение на объект
Снятие информации с каналов утечки
НСД к информации и ресурсам
Способы проникновения
Каналы утечки
Способы НСД
А
О
Э
К
Возможные меры борьбы с угрозами
• СОС
• электронная проходная
• ---------------
• видеонаблюдение
• экранирование
• ---------------
• ---------------
• шифрование
• Разграничение полномочий
• Регистрация событий
• Аутентификация
• Организация доступа в спец. помещения
Политика информационной безопасности

Средства управления информационной безопасностью

Для реализации возложенных на службу информационной безопасности функций в его арсенале должны быть соответствующие средства управления. В идеале они должны объединяться в автоматизированный комплекс обеспечения безопасности (АКБ).

В состав АКБ могут входить:

- система охранной сигнализации (СОС);
- система пожарной безопасности (СПБ);
- телевизионная система наблюдения (ТСН);
- система контроля доступа (СКД).

Автоматизированный комплекс безопасности предназначен для решения следующих задач:

- обнаружения и регистрации фактов несанкционированного проникновения на территорию объекта, в здание и режимные помещения и оповещения службы безопасности о нештатных ситуациях;
- наблюдения за периметром, территорией и особо важными объектами;
- организации доступа и контроля за доступом сотрудников, посетителей и автотранспорта на территорию объекта, а также персонала в режимные, служебные и охраняемые помещения;
- компьютерного анализа безопасности объектов, работоспособности элементов АКБ и действий обслуживающего персонала.

Особенностью комплекса является интегрированность всех систем, позволяющая:

- использовать единые базы данных к конфигурации оборудования, персоналу, событиям, а также единые средства по обеспечению защиты информации;
- реализовать многотерминальный авторизованный доступ пользователей к функциям систем с разграничением прав (администраторы, операторы, охрана и т.д.), парольной защитой и контролем действий;
- создавать и применять единые графические планы;
- на основе модульной открытой архитектуры проектировать и конфигурировать систему под любые требования заказчика, поэтапно наращивать ее информационную и функциональную мощность, а также территориальную распределенность;
- использовать единые средства телекоммуникации, регистрации и печати;
- комплексно использовать оборудование (например, считыватели СКД в СОС для снятия и постановки помещений под охрану);
- взаимодополнять функции систем (например, СОС охранными функциями ТСН или контроль маршрута охраны средствами СКД);
- обеспечить комплексное взаимодействие систем (например, автоматизировать процесс снятия и постановки помещений под охрану на основе информации, получаемой из СКД; управлять режимами работы ТСН по фактам событий, зарегистрированных СОС, СПБ и СКД; управлять состоянием дверей, турникетов по тревогам СОС, СПБ);
- обеспечить автоматизированное или оперативное управление другими службами и устройствами помещений: лифтами, системами оповещения, энергоснабжения, вентиляции, кондиционирования и т.д. на основе информации, получаемой от СКД, СОС и СПБ;
- использовать единую базу событий, а также средства создания и фильтрации отчетов, упростить процесс и повысить достоверность расследования нарушений;
- использовать единую систему бесперебойного энергопитания;
- реализовать комплексную диагностику и обслуживание систем;

- снизить затраты на оборудование, эксплуатацию и обслуживание АКБ.

Программные средства АКБ обеспечивают генерацию следующих видов отчетов:

- о конфигурации системы (устройствах, режимах работы, состояниях датчиков, зон и дверей);
- о местонахождении персонала в конкретный момент, об отработанном времени;
- о действиях оператора;
- о попытках несанкционированного доступа, а также нарушениях в функционировании системы.
- АКБ обеспечивает согласованную работу всех систем безопасности, повышает эффективность работы подразделений безопасности за счет уменьшения времени локализации нарушений, распределяет сообщения системы безопасности по заинтересованным лицам.

Комплекс предусматривает многотерминальный доступ с поддержкой специализированных функций:

- Администратор
- Проходная
- Охрана
- Бюро пропусков.

Заключение

Администратор безопасности является ключевой фигурой в организации защиты КС. Успех масштабного применения СЗИ в организации во многом зависит от наличия развитых средств управления режимами работы различных защитных механизмов. Недостаточное внимание к проблемам обеспечения удобства работы администраторов безопасности по управлению СЗИ на всех этапах жизненного цикла АС часто является основной причиной отказа от использования конкретных СЗИ.

Актуальной задачей является распределение функций между администратором сети и администратором безопасности. Вариант такого распределения представлен на схеме.

Основные функции администратора ОБИ

В функции администратора системы СОБИ входят следующие обязанности:

— гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам;

— управление правами доступа пользователей к ресурсам, согласно выполняемым функциональным задачам;

— управление разрешениями на доступ к ресурсам, предоставляемым пользователям для решения функциональных задач;

— ежедневный анализ регистрационной информации, относящейся к сети в целом и к файловым серверам в особенности;

— оперативная и эффективная реакция на события, содержащие угрозу нарушения функционирования программных и технических средств СОКПП в целом, отдельным ее компонентам, в частности системе ОБИ;

— контроль всех изменений сетевой аппаратно-программной конфигурации;

— регулярное архивирование информации СОБИ;

— контроль работоспособности программных и технических средств СОБИ ЛВС СОКПП, отдельных ее компонентов, устранение возникающих нештатных ситуаций;

— периодический контроль эффективности защиты информации в ЛВС.

Основные мероприятия по обеспечению защиты информации, циркулирующей на объектах СОКПП, от НСД осуществляются в рамках разрабатываемых правил разграничения доступа пользователей и их процессов (программ) к объектам доступа, системным и сетевым ресурсам.