Тип работы: Глава диплома

Предмет: Информатика (другое)

-

ИБ – это процесс обеспечения конфиденциальности, целостности и доступности информации.
Под конфиденциальностью понимается обеспечение доступа к информации только автоматизированным пользователям. Доступность обеспечивает доступ к информации. Под целостностью подразумевается полнота и достоверность информации.
Степень и мера защиты информации применяются к этим трем вышеперечисленным пунктам различно, исходя из того, какую информацию необходимо защищать и степень её секретности.
Главная цель, которую необходимо достигнуть при защите конфиденциальности информации это не дать завладеть ею разного рода конкурентам и злоумышленникам.
Отечественный опыт в защите государственных секретови зарубежный опыт в области защиты интеллектуальной собственности показывает, что результативной может быть только комплексная защита, которая сочетает в себе такие направления защиты, как организованная, инженерно-техническая и правовая.
Для подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, сложилась трехэтапная разработка таких мер.
- оценка угроз;
- анализ уязвимых элементов ИС;
- определение состава средств ИС.
Следующая стадия – определение защитных способов,которые включают ответы на следующие вопросы:
- какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?
- какие угрозы должны быть устранены и в какой мере?
- какие ресурсы системы должны быть защищаемы и в какой степени?
- с помощью каких средств должна быть реализована защита?
Можно сформулировать основные требования к системе защиты информации.
1. Система защиты информации должна быть представлена как нечто целое. Целостность системы будет выражаться в наличии единой цели ее функционирования, информационных связей между элементами системы, иерархичности построения подсистемы управления системой защиты информации.
2. Система защиты информации должна обеспечивать безопасность информации, средств информации, защиту интересов участников информационных отношений и невозможность несанкционированного доступа злоумышленника к защищаемой информации.
3. Система защиты информации в целом, применяемые методы и средства защиты должны быть по возможности прозрачными для законного пользователя, не создавать ему больших дополнительных неудобств, связанных с процедурами доступа к информации.

1.2 Организационно-правовое обеспечение информационной безопасности.
Организационно-правовое обеспечение ИБ представляет собою совокупность решений, законов, нормативов, регламентирующих, как общую организацию работ по обеспечению ИБ, но и создание и функционирование систем защиты информации на конкретных объектах. Основные функции организационно-правовой базы следующие.
1. Разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации.
2. Определение системы органов и должностных лиц, ответственных за обеспечение ИБ в стране и порядка регулирования деятельности предприятия и организации в этой области.
3. Создание полного комплекса нормативно-правовых руководящих и методических документов, регламентирующих вопросы обеспечения ИБ как в стране в целом, так и на конкретном объекте.
4. Определение мер ответственности за нарушения правил защиты.

5. Определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.
Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи. При этом различают признаки защищаемой информации:
- засекречивать информацию, т. е. ограничивать к ней доступ, может только ее собственник или уполномоченные им на то лица;
- чем важнее для собеседника информация, тем тщательнее он её защищает, а для того чтобы все, кто сталкивается с этой защищаемой информацией знали, что одну информацию необходимо оберегать более тщательней, чем другую, собственник определяет ей различную степень секретности;
- защищаемая информация должна приносить определенную пользу её собственнику и оправдывать затрачиваемые на её защиту силы и средства;
- секретная информация обладает определенным генетическим свойством: если эта информация является основанием для создания новой информации, то созданная на этой основе информация является, как правило, секретной.
Отличительным признаком защищаемой информации является то, что засекречивать ее может только собственник или уполномоченные им на то лица.
1.3 Инженерно-техническая защита информации
ИТЗ – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.
Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некой системы классификаций.
Многообразие классификационных характеристик позволяет рассматривать средства ИТЗ к объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны служб безопасности.
Основная классификация ИТЗ – по функциональному назначению средств ИТЗ.
Очевидно, что такое деление средств защиты информации условно, т. к. они часто взаимодействуют и реализуются в комплексе в виде аппаратно-программных модулей с широким использованием алгоритмов закрытия информации.
1.3.1 Физические свойства защиты
Для создания различных препятствий на пути движения злоумышленников используются разнообразные устройства, приспособления, конструкции, аппарата, изделия, которые называются физическими средствами защиты информации (Системы ограждений и физической изоляции, системы контроля доступа, и запирающие устройства и хранилища).
К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа, проноса и выноса средств и материалов, и других возможных видов преступных действий.
Эти средства применяются для решения следующих задач:
- охрана территории предприятия и наблюдения за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещение.
Все физические средства защиты объектов можно разделить на три категории:
- средства предупреждения (заборы вокруг объектов);
- средства обнаружения (охранная сигнализация, охранное телевидение и др.);
- системы ликвидации угроз (средства пожаротушения).

-