Основы ИБ (КБ-201, 202; 2021г.)

Лекция 2. Основные понятия ИБ. Комплексный подход к защите информации

Безопасность информации - состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

Конфиденциальность, доступность и целостность представляют собой три наиболее важных свойства (аспекты) информации в рамках обеспечения ее безопасности:

конфиденциальность информации - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

доступность информации - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Выделяются следующие **направления** защиты информации (лекция 1):

- **правовая защита информации** — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- **физическая защита информации** — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

- **техническая защита информации** — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- **криптографическая защита информации** — защита информации с помощью ее криптографического преобразования.

Системный подход – это принцип рассмотрения проекта, при котором анализируется система в целом, а не её отдельные части. Его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Это объясняется тем, что, как показывает практика, улучшение одних параметров часто приводит к ухудшению других, поэтому необходимо стараться обеспечить баланс противоречий требований и характеристик.

«**Комплексная система защиты информации** – это система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации».

Следовательно, только комплексная система может гарантировать достижение максимальной эффективности защиты информации, поскольку системность обеспечивает необходимые составляющие защиты и устанавливает между ними логическую и технологическую связь, а комплексность, требует полноты этих составляющих, всеохватности защиты, обеспечивает ее надежность.

Примеры проявления комплексности в защите информации

Виды направлений защиты информации: правовая, организационная, техническая, криптографическая.

Аспекты ИБ: конфиденциальность, целостность, доступность.

Построение системы защиты информации: анализ, разработка системы защиты (планирование), реализация СЗИ, сопровождение СЗИ.

Отношение к объекту защиты: АРМ, сеть, помещение (здание, территория).

Возможные события: безотказное функционирование СЗИ, отказ (нарушение), оценка ущерба, меры по ликвидации, резервирование, восстановление СЗИ.

Деятельность в области защиты информации: ЗИ, производство СЗИ, сертификация СЗИ, услуги по ЗИ, лицензирование деятельности по ЗИ, аттестация объектов информатизации по требованиям безопасности информации.

И др.

Принципы построения комплексной системы защиты информации

В процессе развития научных и практических работ по защите информации наряду с конкретными разработками конкретных вопросов защиты формировались и развивались и общеметодологические принципы (общие положения) построения и функционирования КСЗИ. Соблюдение требований выполнения таких принципов в общем случае способствует повышению эффективности защиты информации на предприятии.

Ниже перечисленные принципы относятся к любому предприятию: государственному, коммерческому, смешанному и другим формам собственности, а также большим, средним, малым**. Среди принципов выделяют:**

1. Принцип законности. Здесь меры обеспечения функционирования предприятия разрабатываются на основе и в рамках действующих правовых актов. Правовые акты предприятия не должны противоречить государственным законам и подзаконным актам;

2. Принцип превентивности, т.е. упреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз. На основе анализа этих угроз вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз, т.е. разрабатываются упреждающие мероприятия;

3. Принцип полноты состава защищаемой информации. Он заключается в том, что защите подлежит не только информация, содержащая государственную, коммерческую или служебную тайну, но даже часть служебной информации, утрата которой может нанести ущерб ее собственнику;

4. Принцип обоснованности защиты информации. Выполнение этого принципа заключается в установлении целесообразности засекречивания и защиты той или другой информации с точки зрения экономических и иных последствий такой защиты. Это позволяет расходовать средства на защиту только той информации, утрата или утечка которой может нанести действительный ущерб ее владельцу;

5. Принцип персональной ответственности за защиту информации. Заключается в том, что каждый сотрудник предприятия персонально отвечает за сохранность и неразглашение вверенной ему защищаемой информации, а за утрату или распространение такой информации несет уголовную, административную или иную ответственность;

6. Принцип непрерывности, т.е. защита информации происходит на регулярной основе (постоянно);

7. Принцип гибкости, т.е. это возможность варьирования и замены элементов системы без нарушения структуры и функционирования;

8. Принцип концептуального единства. В комплексных системах защиты архитектура, технология, организация и обеспечение функционирования, как в целом, так и в отдельных ее компонентах должны рассматриваться в соответствии с общей концепцией защиты информации и теми требованиями, которые предъявляются для данной системы;

9. Принцип регламентации предоставляемых прав, т.е. каждый сотрудник предприятия имеет доступ только к определенной информации, которая ему действительно необходима для выполнения своих функций в процессе работы, причем предоставленные права должны быть заранее определены и утверждены в установленном порядке, например, в договоре при приеме на работу;

10. Принцип активности. Здесь меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений и служб предприятия, отдельных лиц, а также установления необходимых контактов с внешними организациями, способными оказать комплексной защите информации необходимое содействие в обеспечении безопасности предприятия.

11. Принцип плановой основы деятельности предприятия. Здесь деятельность по обеспечению защиты информации должна строиться на основе комплексной программы обеспечения защиты информации на предприятии, разрабатываются подпрограммы обеспечения этой защиты по основным его видам (экономической, техногенной, научно-технической, экологической, технологической, информационной, психологической, физической, пожарной и другим видам), а также разрабатываются для их исполнения планы работы подразделений предприятия и отдельных сотрудников;

12. Принцип системности. Этот принцип предполагает учет всех факторов, влияющих на организацию КСЗИ предприятия. При этом должны быть охвачены все этапы и режимы функционирования, задействованы все силы и средства.

Среди рассмотренных принципов едва ли можно выделить более или менее важные. А при построении КСЗИ важно использовать их в совокупности.

Таким образом, учитывая многообразие потенциальных угроз информации на предприятии, сложность его структуры, а также участие человека в технологическом процессе обработки информации цели защиты информации могут быть достигнуты только путем создания СЗИ на основе ***комплексного подхода.***

А это одновременно подразумевает, что **защита информации** – есть непрерывный процесс, который заключается в контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

Учитывая все вышесказанное можно сформулировать четыре пункта постулата системы защиты:

1. Система защиты информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая;

2. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

3. Никакую систему защиты нельзя считать абсолютно надежной, т.к. всегда может найтись злоумышленник, который найдет лазейку для доступа к информации (действия злоумышленника всегда носят комплексный характер, т.к. он любыми средствами стремится добыть важную информацию);

4. Система защиты должна быть адаптируемой (приспособляющейся) к изменяющимся условиям.

Важной частью СЗИ является ***комплекс организационных мер*** по защите информации.

Организационные меры защиты информации представляют собой комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем). К основным организационным мероприятиям относятся:

создание службы защиты информации;

разработка организационно-распорядительных документов, необходимых для организации комплексной защиты информации;

определение порядка доступа к защищаемым объектам;

установление и оформление правил разграничения доступа;

ознакомление сотрудников организации с перечнем защищаемой информации, организационно-распорядительной документации по работе с ней;

обеспечение охраны объекта информатизации путем установления системы контроля доступа, постов охраны, ограждающих сооружений и т.п.

управление системой защиты информации.

Состав организационно-распорядительных документов, как правило, включает:

перечень информации, подлежащей защите;

документы, регламентирующие порядок обращения сотрудников предприятия с информацией, подлежащей защите;

положения о структурных подразделениях предприятия;

документы, регламентирующие порядок взаимодействия предприятия со сторонними организациями по вопросам обмена информацией;

документы, регламентирующие порядок эксплуатации автоматизированных систем предприятия;

планы защиты автоматизированных систем предприятия;

документы, регламентирующие порядок разработки, испытания и сдачи в эксплуатацию программных средств;

документы, регламентирующие порядок закупки программных и аппаратных средств (в т.ч. средств защиты информации);

документы, регламентирующие порядок эксплуатации технических средств связи и телекоммуникации.

Помимо этого, СТР-К для обеспечения защиты конфиденциальной информации **рекомендует следующее**:

на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;

в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;

по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;

изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;

при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

Все носители информации, используемые в технологическом процессе обработки информации, подлежат учету в том подразделении, которое является владельцем АС, обрабатывающей эту информацию. Учет можно осуществлять по карточкам, бумажным журналам или автоматизировано. Носители должны быть промаркированы. Маркировка должна содержать:

учетный номер носителя
дата
гриф секретности
номер экземпляра
подпись сотрудника, ответственного за ведение учета.

Ответственность за соблюдением в организации или компании организационных (административных) мер по защите информации лежит на руководителе, начальнике службы безопасности (информационной безопасности), системном (сетевом) администраторе.