

Глава 2

Концепция построения системы безопасности предприятия

1. Общая характеристика организационных методов защиты информации
2. Требования к построению систем безопасности предприятия
3. Концептуальная модель информационной безопасности
4. Виды объектов защиты
5. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии
6. Основные направления организационной защиты информации на предприятии

1. Общая характеристика организационных методов защиты информации

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня её безопасности.

Организационная защита информации – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации.

2. Требования к построению систем безопасности предприятия

При построении системы безопасности следует учитывать следующие рекомендации:

- Обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме.
- Безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты и противодействия во всех структурных элементах производственной системы и на всех этапах технологического цикла. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм – ***систему безопасности предприятия (СБП)***.
- Никакая СБП не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала предприятия и пользователей, соблюдения ими всех установленных правил, направленных на обеспечение безопасности.

Основные задачи системы безопасности

Задачи

```
graph TD; A[Задачи] --> B[своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия]; A --> C[отнесение информации к категории ограниченного доступа]; A --> D[создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия]; A --> E[создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей];
```

своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия

отнесение информации к категории ограниченного доступа

создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия

создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей

Принципы организации и функционирования системы безопасности

1. Комплексность

2. Своевременность

3. Непрерывность

4. Активность

5. Законность

6. Обоснованность

7. Экономическая целесообразность

8. Специализация

9. Взаимодействие и координация

10. Совершенствование

11. Централизация управления

Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных

Совершенствование. Предусматривает совершенствование меры

Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности.

3. Концептуальная модель информационной безопасности И

Угрозы И

Цели угроз

- ознакомление
- модификация
- уничтожение

Способы НСД

Угрозы

- целостности
- конфиденциальности
- полноте
- доступности

Источники угроз

- конкуренты
- преступники
- коррупционеры

Рубеж

Защиты И

Защита И

Направления
защиты
Правовое
организационное
техническое

Объект защиты

- Сведения о составе, состоянии и деятельности предприятия

Способы защиты
упреждение
предотвращение
пресечение
противодействие

И

Источники И

- люди
- документы
- технические носители
- технические средства
- продукты
- публикации
- отходы

Средства защиты
физические
программные
аппаратные
инженерно-тех.
криптографические

Трёхмерная модель комплексной безопасности



4. Виды объектов защиты

Объекты защиты

руководящие
работники и
производственный
персонал,
владеющий
информацией
ограниченного
пользования

серийно
выпускаемая
продукция и
опытные
образцы

финансовые
средства и
документы

информационные
ресурсы с
ограниченным
доступом,
составляющие
служебную и
коммерческую
тайну

материальные
ценности

технические,
программно-
аппаратные
средства защиты
информации и
различные
системы охраны и
защиты
материальных и
информационных
ресурсов

средства
производства и
производственные
ресурсы

средства и
автоматизированные
системы обработки
информатизации

5. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии

Под **угрозой** или **опасностью утраты информации** понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Виды угроз информации



Возможные пути утраты информации



6. Основные направления организационной защиты информации на предприятии

Система защиты информации — это рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Основные элементы системы защиты предприятия



Правовой элемент

- наличие в организационных документах предприятия, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;
- формулирование и доведение до сведения всех сотрудников предприятия (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
- разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Организационный элемент

- порядка защиты информации при проведении совещаний, заседаний,
- перерывов, приема посетителей, работ по предоставлению срочных
- агентств, средств массовой информации; перечня защищаемой информации
- составления и регулярного обновления; обеспечения и составления поведения персонала, защищаемых для работы с конфиденциальной информацией, документированных технических систем и
- средств защиты информации и охраны, сертификации информационных систем, наличия разрешительной системы разграничения доступа персонала к системам, предназначенных для обработки защищаемой информации;
- пропускного режима на территории, в здании, в помещениях предприятия, использования методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;
- системы охраны территории, здания, помещений, оборудования, транспорта и формирования направлений и методов воспитательной работы с персоналом и персонала предприятия; контроля соблюдения сотрудниками порядка защиты информации;
- действий персонала в экстремальных ситуациях;
- технологий защиты, обработки и хранения бумажных, машиночитаемых и
- электронных документов, приобретения (доставки) видеокассет, аудиотехнических средств защиты информации, внемашиной технологии
- защиты электронных документов; персональных компьютеров,
- информации сетей локальных сетей предприятия от случайных или
- работ по управлению системой защиты информации персонала;
- критериев и порядка проведения оценок мероприятий по установлению степени эффективности системы защиты информации.

Инженерно-технический элемент

- сооружения инженерной защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);
- средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т.п.;
- средства защиты помещений от визуальных способов технической разведки;
- средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, охранной и пожарной сигнализации);
- средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.).

Программно-аппаратный элемент

- автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;
- программы защиты информации, работающие в комплексе с программами обработки информации;
- программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.).

Криптографический элемент

- регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;
- определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;
- регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радио связи;
- регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;
- регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Контрольные вопросы

1. Что включают организационные методы защиты информации?
2. На что направлена деятельность по защите информации?
3. Какие задачи обеспечения информационной безопасности решаются на организационном уровне?
4. Что такое система безопасности предприятия?
5. На основе каких принципов осуществляется функционирование системы безопасности предприятия?
6. Каким требованиям должна удовлетворять система безопасности предприятия?
7. Что является компонентами комплексной модели информационной безопасности?
8. Перечислите виды объектов защиты.
9. Назовите возможные пути утраты информации.
10. Дайте характеристику основным элементам системы защиты предприятия.