ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

КОЛЛЕДЖ СВЯЗИ №54

«Основы информационной безопасности»

Тема: Организационные основы защиты информации

Роль и место организационной защиты информации

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации. От полноты и качества решения организационных задач зависит эффективность функционирования системы защиты информации в целом.

Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации, определяются ***исключительной важностью принятия своевременных и верных управленческих решений с учетом имеющихся сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.***

Основные направления деятельности по ОЗИ

1. Планирование мероприятий по защите информации и персональный контроль за их выполнением;
2. Принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций;
3. Распределение обязанностей и задач между должностными лицами и структурными подразделениями;
4. Аналитическая работа и т.д.

Цель принимаемых организационных мер - исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения ущерба, к которому эта утечка может привести.

Два определения ОЗИ

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

(показывает сущность организационной защиты информации)

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

(раскрывает структуру ОЗИ на уровне предприятия)

1. Принцип комплексного подхода - эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации

2. Принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

3. Принцип персональной ответственности - наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Основные условия ОЗИ

1. Непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;

2. Неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

Силы и средства ЗИ

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, — ***совокупность сил и средств предприятия, используемых для организации защиты информации***.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования.

Ведущую роль в организации защиты информации на предприятии играют *руководитель предприятия*, а также *его заместитель*, непосредственно возглавляющий эту работу.

Органы защиты информации

А) Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, создают ***самостоятельные структурные подразделения*** и используют высокоэффективные СЗИ.

Б) Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу ее небольших объемов, вместо создания подразделений они могут включать в свои штаты ***отдельные должности специалистов*** по защите информации.

Данные подразделения и должности являются ***органами защиты информации.***

Обязанности руководителя предприятия по ЗИ

Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.

Он обязан:

1. Знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации.

Обязанности руководителя предприятия по ЗИ

2. Определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области.

3. Проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации.

4. Оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

Обязанности заместителя руководителя предприятия по ЗИ

Заместитель руководителя предприятия **обязан**:

1.Постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации.

2. Руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации).

3. Выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

Виды структурных подразделений

На предприятиях для организации работ по защите информации могут создаваться следующие основные ***виды структурных подразделений:***

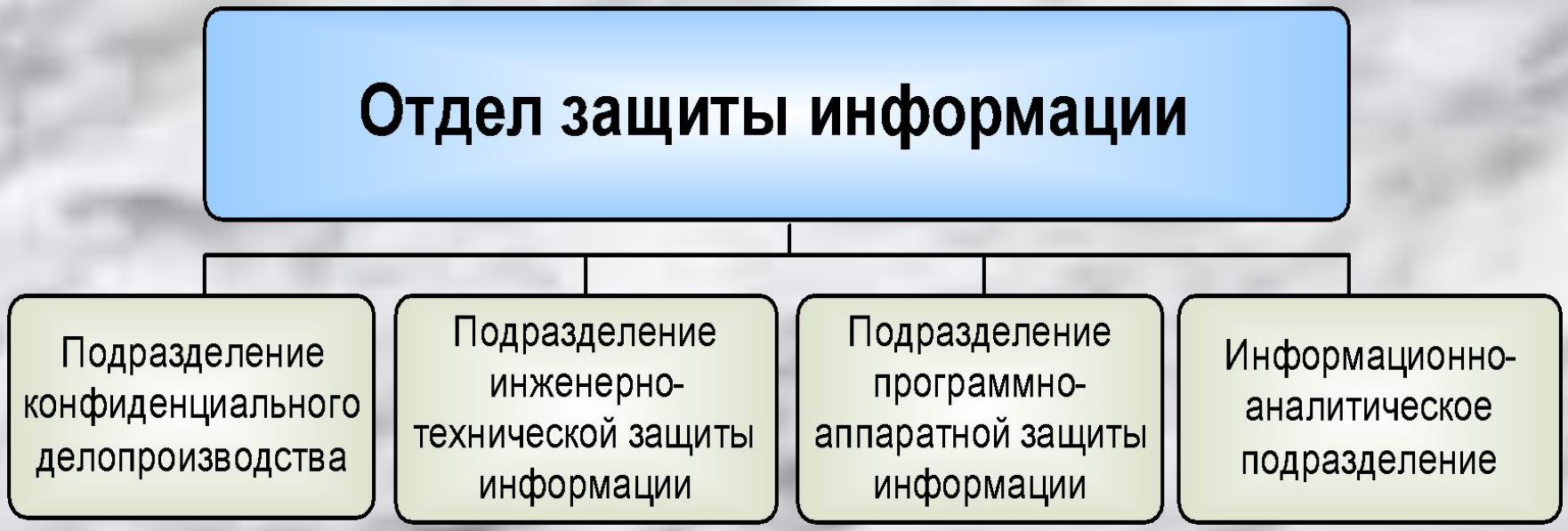
- режимно-секретные;
- подразделения по технической защите информации и противодействию иностранным техническим разведкам;
- подразделения криптографической защиты информации;
- мобилизационные;
- подразделения охраны и пропускного режима.

По решению руководителя предприятия данные подразделения организационно могут объединяться в ***службу безопасности***, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия.

Подразделение охраны и пропускного режима создается в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Вариант структуры отдела ЗИ



Подразделение конфиденциального делопроизводства

- Обработка (получение, классификация, учет, рассылка) и хранение конфиденциальных документов.
- Контроль системы конфиденциального документооборота

Подразделение инженерно-технической информации

Инженерно-техническая защита информации предназначена для активно-пассивных противодействий средствам технической разведки и формирования рубежей охраны территории, зданий, помещений, оборудования с помощью комплексов технических средств и **включает себя**:

1. Сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здания и помещения.

Подразделение инженерно-технической защиты информации

2. Средства защиты технических каналов утечки информации при работе ЭВМ, средств связи, других приборов и офисного оборудования, при проведении совещаний, беседах с посетителями и сотрудниками.

3. Средства защиты помещений от визуальных способов технической разведки.

4. Средства обеспечения охраны территорий, зданий, помещений.

5. Средства противопожарной охраны.

6. Технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, дискет, дисков и других носителей информации.

Целями защиты информации, обрабатываемой и хранимой в ПЭВМ, являются:

1. Предотвращение потери и утечки информации, перехвата и вмешательства злоумышленника на всех уровнях обработки данных и для всех объектов.

2. Обеспечение целостности данных на всех этапах их преобразования и сохранности средств программного обеспечения.

Задачи подразделения программно-аппаратной ЗИ:

- предотвращение несанкционированного доступа (НСД) к информации;
- предотвращение утечки информации за счет ПЭМИН;
- защита информации от компьютерных вирусов;
- защита информации от сбоев в системе питания;
- защита от копирования;
- программная защита каналов передачи данных.

Информационно-аналитическое подразделение

- сбор и оперативное использование информации по гражданскому, уголовному и хозяйственному законодательству;
- подготовка и анализ заключаемых договоров, а также подготовка рекомендаций по вопросам правовой защиты от противоправных действий;
- сбор, накопление, обработка, анализ и выдача информации о возможных клиентах и партнерах, перспективах сотрудничества;
- работа с вкладчиками, акционерами, финансовыми брокерами и дилерами с использованием методов экономической разведки;
- подготовка и проведение рекламных кампаний;

- сбор и анализ коммерческой информации, в явном или неявном виде присутствующей в средствах массовой информации;

- сбор информации по конкурирующим фирмам, а также составление психологических портретов их лидеров;

- сбор информации о процессах, происходящих в криминальных структурах, о криминогенной обстановке в районе деятельности фирмы;

- выработка рекомендаций и мер противодействия преступным посягательствам, направленным против банка (фирмы) и их сотрудников.

Нештатные структуры службы безопасности

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства и службы безопасности могут создаваться ***отдельные комиссии***, выполняющие определенные контрольно-ревизионные функции на временной или постоянной основе.

1. Квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей)

2. Комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.

3. Периодические проверочные комиссии для проверки знаний и умения выполнять требования нормативных документов по защите банковской тайны, а также для оценки эффективности и надежности защитных мероприятий по обеспечению безопасности

4. Специальные группы по аудиту безопасности организации