ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Организационные основы защиты информации на предприятии

Федоров Дмитрий Николаевич
dnf@dnf.su

РАЗДЕЛЫ ТЕМЫ

- Основные направления, принципы и условия организационной защиты информации
- Основные подходы и требования к организации системы защиты информации
- Основные методы, силы и средства, используемые для организации защиты информации

Раздел 1

ОСНОВНЫЕ НАПРАВЛЕНИЯ, ПРИНЦИПЫ И УСЛОВИЯ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ВВЕДЕНИЕ

- Из упоминавшихся ранее средств и методов обеспечения **информационной безопасности** особо были выделены организационные, которые в совокупности с другими элементами системы **защиты информации** на предприятии подробно описаны в последующих главах учебника.
- Для наиболее полного и глубокого анализа происходящих в сфере **защиты конфиденциальной информации** процессов, понимание сущности планируемых и проводимых в этих целях мероприятий прежде всего необходимо рассмотреть одно из важнейших направлений **защиты конфиденциальной информации** — **организационную защиту информации.**
- Среди основных направлений защиты информации наряду с организационной выделяют **правовую и инженерно-техническую защиту информации**. Однако организационной защите информации среди этих направлений отводится особое место.

РОЛЬ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ

- **Организационная защита информации** является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия.
- От полноты и качества решения руководством предприятия и должностными лицами 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 предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов **защиты информации** и на основе действующего нормативно-методического аппарата.

ЗАДАЧА ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ

- **Организационная защита информации** призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации.
- Данные меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

РОЛЬ РУКОВОДСТВА ПРЕДПРИЯТИЯ

- Основными направлениями деятельности, осуществляемой руководителем предприятия по защите информации, являются:
  - планирование мероприятий по **защите информации** и персональный контроль за их выполнением,
  - принятие решений о непосредственном доступе к **конфиденциальной информации** своих сотрудников и представителей других организаций,
  - распределение обязанностей и задач между должностными лицами и структурными подразделениями,
  - аналитическая работа и т.д.
- Цель принимаемых руководством предприятия и должностными лицами организационных мер — **исключение утечки информации** и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

- **Система мер по защите информации** в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.
- Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ «ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ»

- Используются два примерно равнозначных определения организационной **зашиты информации**.
  - **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**.
  - **Организационная защита информации** на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.
- Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе — раскрывает ее структуру на уровне предприятия.
- Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов **защиты информации** наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств

ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ

- Основные направления
- Основные принципы
- Основные условия

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОРГАНИЗАЦИОННОЙ **ЗАЩИТЫ** ИНФОРМАЦИИ

- Организация работы с персоналом;
- Организация внутриобъектового и пропускного режимов и охраны;
- Организация работы с носителями сведений;
- Комплексное планирование мероприятий по защите информации;
- Организация аналитической работы и контроля.

ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- 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;
- 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);
- 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 ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;
- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Раздел 2

ОСНОВНЫЕ ПОДХОДЫ И ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

РЕШЕНИЕ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

- Успешное решение комплекса задач **по защите информации** не может быть достигнуто без создания единой основы, так называемого «активного кулака» предприятия, способного концентрировать все усилия и имеющиеся ресурсы для исключения утечки **конфиденциальной информации** и недопущения возможности нанесения ущерба предприятию.
- Таким «кулаком» призвана стать **система защиты информации** на предприятии, создаваемая на соответствующей нормативно-методической основе и отражающая все направления и специфику деятельности данного предприятия.
- Под **системой защиты информации** понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.

ОСНОВНЫЕ ПОДХОДЫ: АНАЛИЗ

- Для решения организационных задач по созданию и обеспечению функционирования **системы защиты информации** используются несколько основных подходов, которые вырабатываются на:
  - основе существующей нормативно-правовой базы и
  - с учетом методических разработок по тем или иным направлениям **защиты конфиденциальной информации**.
- Один из основных подходов к созданию **системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия** с учетом устремленности конкурирующих организаций к овладению **конфиденциальной информацией** и, тем самым, нанесению ущерба предприятию.
- Важным элементом анализа является работа по определению **перечня защищаемых информационных ресурсов** с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

ОРГАНИЗАЦИЯ РАБОТЫ ПО АНАЛИЗУ

- Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности.
- Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

ЧТО НЕОБХОДИМО УЧЕСТЬ ПРИ АНАЛИЗЕ

- При создании системы защиты информации, в первую очередь, учитываются:
  - наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания.
  - новые, перспективные направления деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность
  - развивающиеся международные связи.
- В соответствии с названными приоритетами:
  - Формируется перечень возможных угроз информации, подлежащей защите.
  - Определяются конкретные силы, средства, способы и методы ее защиты.

СИСТЕМНЫЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ

- централизованность — обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;
- плановость — объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;
- целенаправленность — рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;
- активность — обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;
- надежность и универсальность — охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

Раздел 3

ОСНОВНЫЕ МЕТОДЫ, СИЛЫ И СРЕДСТВА, ИСПОЛЬЗУЕМЫЕ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

СИЛЫ И СРЕДСТВА

- 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.
  - Предприятия, работающие с **конфиденциальной информацией** и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации.
  - 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, или,** на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области.
- Данные подразделения и должности являются органами защиты информации.

КТО ОРГАНИЗУЕТ РАБОТУ ПО ЗАЩИТЕ ИНФОРМАЦИИ

- Руководитель предприятия
- Заместитель руководителя, непосредственно возглавляющий эту работу
- Структурные подразделения, организующие и проводящие данную работу.

Далее рассмотрим особенности работы данных лиц и подразделений

РУКОВОДИТЕЛЬ ПРЕДПРИЯТИЯ

- 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:
  - знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
  - определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
  - проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;
  - оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ ПРЕДПРИЯТИЯ

- Заместитель руководителя предприятия обязан:
  - постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации;
  - руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации);
  - выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

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.

Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

Первые три вида подразделений создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).

По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.

РЕЖИМНО-СЕКРЕТНОЕ ПОДРАЗДЕЛЕНИЕ

- Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению **защиты сведений**, составляющих государственную тайну.
- На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создается и функционирует служба безопасности (служба защиты информации).

ПОДРАЗДЕЛЕНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ

- Подразделение по технической **защите информации** и противодействию иностранным техническим разведкам решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к **конфиденциальной информации** и подлежащих защите.
- Подразделение **криптографической защиты информации** создается в целях предотвращения **утечки конфиденциальной информации** при ее передаче по открытым каналам (линиям) связи с помощью технических средств, а также при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

ПОДРАЗДЕЛЕНИЕ ОХРАНЫ И МОБИЛИЗАЦИОННОЕ ПОДРАЗДЕЛЕНИЕ

- 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. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.
- Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

ИНЫЕ СТРУКТУРНЫЕ ПОДРАЗДЕЛЕНИЯ

- Для иных привлекаемых структурных подразделений выполнение мероприятий по защите информации не является основной функцией:
  - кадровый орган,
  - орган юридической службы (юрисконсульт),
  - орган психологической и воспитательной работы,
  - пресс-служба предприятия и др.
- Для проведения работ по организации **защиты информации** используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области:
  - постоянно действующая техническая комиссия
  - экспертная комиссия
  - комиссия по рассекречиванию носителей **конфиденциальной информации**,
  - комиссия по категорированию объектов информатизации и др.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

- Для максимальной эффективности решения задач **защиты информации**, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии **средства защиты информации.**
- Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

ТИПЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

- **Технические средства защиты информации** — устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.
- **Криптографические средства защиты информации** — средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).
- **Программные средства защиты информации** — системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих **сил и средств**.
- Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют **методы защиты информации**, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.
- **Методы защиты информации** — применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

ВИДЫ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

- Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.
- Правовые методы регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, ее организационные направления.
  - Тесную связь организационных и правовых **методов защиты информации** можно показать на примере решения задач по **исключению утечки конфиденциальной информации**, в частности относящейся к коммерческой тайне предприятия, при его взаимодействии с различными государственными и территориальными инспекторскими и надзорными органами. Эти органы в соответствии с предоставленными им законом полномочиями осуществляют деятельность по получению (истребованию), обработке и хранению информации о предприятиях и гражданах (являющихся их сотрудниками).
  - Передача информации, в установленном порядке отнесенной к коммерческой тайне или содержащей персональные данные работника предприятия, должна осуществляться на основе договора, предусматривающего взаимные обязательства сторон по нераспространению (неразглашению) этой информации, а также необходимые меры по ее защите.

ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕТОДЫ

- **Организационные механизмы защиты информации** определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.
- **Технические методы защиты информации**, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при ее хранении, накоплении и обработке с использованием средств автоматизации. Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях.

ОРГМЕТОДЫ И РЕШАЕМЫЕ ИМИ ЗАДАЧИ

- реализация на предприятии эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение ее утечки;
- осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту конфиденциальной информации;
- определение перечней сведений, относимых на предприятии к различным категориям (видам) конфиденциальной информации;
- ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени ее конфиденциальности;
- подбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение и воспитание персонала предприятия, допущенного к конфиденциальной информации;
- организация и ведение конфиденциального делопроизводства;
- осуществление систематического контроля за соблюдением установленных требований по защите информации.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru