Информационная безопасность государства (РФ)

Тема 1.1 Введение в правовое обеспечение информационной безопасности

УД «Организационно-правовое обеспечение информационной безопасности»

Преподаватель: Бояркин Д.В.

Введение

- Наряду с политической, экономической, военной, социальной и экологической безопасностью составной частью национальной безопасности Российской Федерации является информационная безопасность.
- Под информационной безопасностью Российской Федерации понимается состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Введение

- Информационная сфера представляет собой совокупность информационных ресурсов и информационной инфраструктуры объекта защиты.
- Совокупность хранимой, обрабатываемой и передаваемой информации, используемой для обеспечения процессов управления, называют информационным ресурсом.

Введение

К информационным ресурсам относятся:

- информационные ресурсы предприятий оборонного комплекса, содержащие сведения об основных направлениях развития вооружения, о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов;
- информационное обеспечение систем управления и связи;
- информация о фундаментальных и прикладных НИР, имеющих государственное значение и др.

Введение

- Информационная инфраструктура – это совокупность информационных подсистем, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации.

Информационная инфраструктура включает:

- информационную инфраструктуру центральных, местных органов государственного управления, научно-исследовательских учреждений;
- информационную инфраструктуру предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления и связи.

Угрозы ИБ

- Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.
- Угрозы информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

Угрозы ИБ

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения, являются:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети);
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Угрозы ИБ

К внутренним угрозам, которые будут представлять особую опасность в условиях обострения военно-политической обстановки, относятся:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях силовых структур Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж силовых структур Российской Федерации и их боеготовность;
- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

Угрозы ИБ

К угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем относятся:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;

Угрозы ИБ

К угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем относятся:

- утечка информации по техническим каналам;
- внедрение электронных устройств, предназначенных для перехвата информации, в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Направления развития системы ИБ РФ

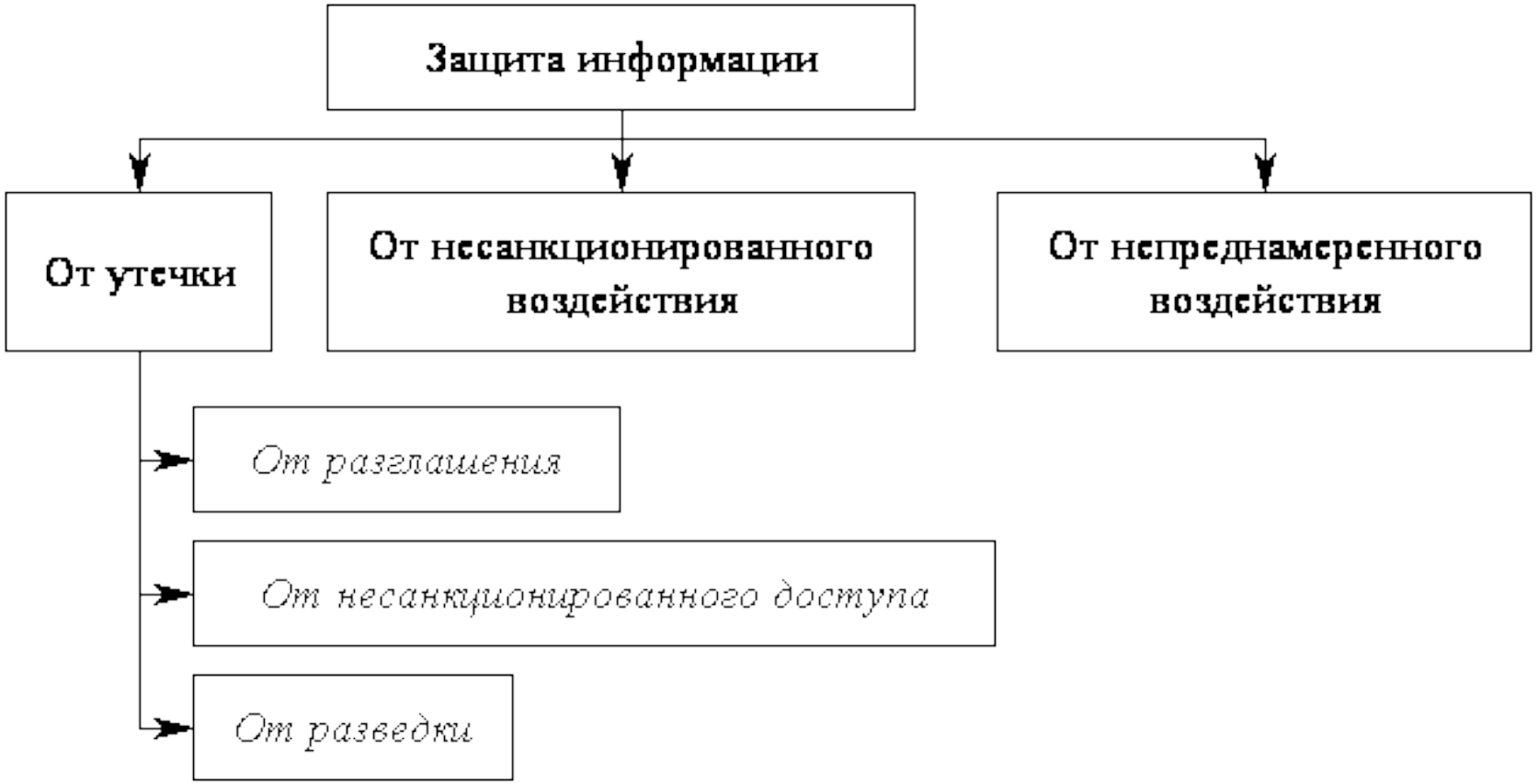
Основными направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления и связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации, развитие защищенных систем связи и управления, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы, координация их взаимодействия.

Защита информации в РФ

- *Оценка состояния информационной безопасности базируется на анализе источников угроз (потенциальной возможности нарушения защиты).*
- *Деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на нее, называют защитой информации. Объектом защиты является информация или носитель информации, или информационный процесс, которые нужно защищать.*
- *Защита информации организуется по трем направлениям: от утечки, от несанкционированного воздействия и от непреднамеренного воздействия*

Защита информации в РФ



Защита информации в РФ

- **Первое направление** – защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.
- Защита информации от разглашения направлена на предотвращение несанкционированного доведения ее до потребителя, не имеющего права доступа к этой информации.
- Защита информации от несанкционированного доступа направлена на предотвращение получения информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа физических лиц, в том числе общественная организация; отдельное физическое лицо.
- Защита информации от технической разведки направлена на предотвращение получения информации разведкой с помощью технических средств.

Защита информации в РФ

- **Второе направление** – защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.
- **Третье направление** – защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате уничтожению или сбою функционирования носителя информации.
- **Организовать защиту информации** – значит создать систему защиты информации, а также разработать мероприятия по защите и контролю эффективности защиты информации.


Организация защиты информации
Система защиты информации
Мероприятия по защите информации
Мероприятия по контролю эффективности защиты информации
Орган и (или) исполнители
Объект защиты информации
Техника защиты информации
Способ защиты информации
Категорирование защищаемой информации
Лицензирование
Сертификация
Аттестация
Способ контроля эффективности защиты информации
Контроль состояния защиты информации
Средство защиты информации
Средство контроля эффективности защиты информации
Средства и системы управления
Контроль организации защиты информации
Контроль эффективности защиты информации
Организационный
Технический