Информационная безопасность

Лекция 14 Комплексная модель безопасности

В. М. Куприянов, Национальный центр ИНИС МАГАТЭ, НИЯУ МИФИ

НЦ ИНИС МИФИ

Литература

Основная литература для изучения дисциплины:

- Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности.- М.: Горячая линия – Телеком, 2006.
- Петраков А.В. Основы практической защиты информации.- М.: Радио и связь, 2001.
- Шумский А.А., Шелупанов А.А. Системный анализ в защите информации.- М.: Гелиос АРВ, 2005.
- Герасименко В.А., Малюк А.А. Основы защиты информации.- М.: Инкомбук, 1997.
- Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.- М.: Энергоатомиздат, 1994.
- Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации.- Орел: ОВИПС, 2000.

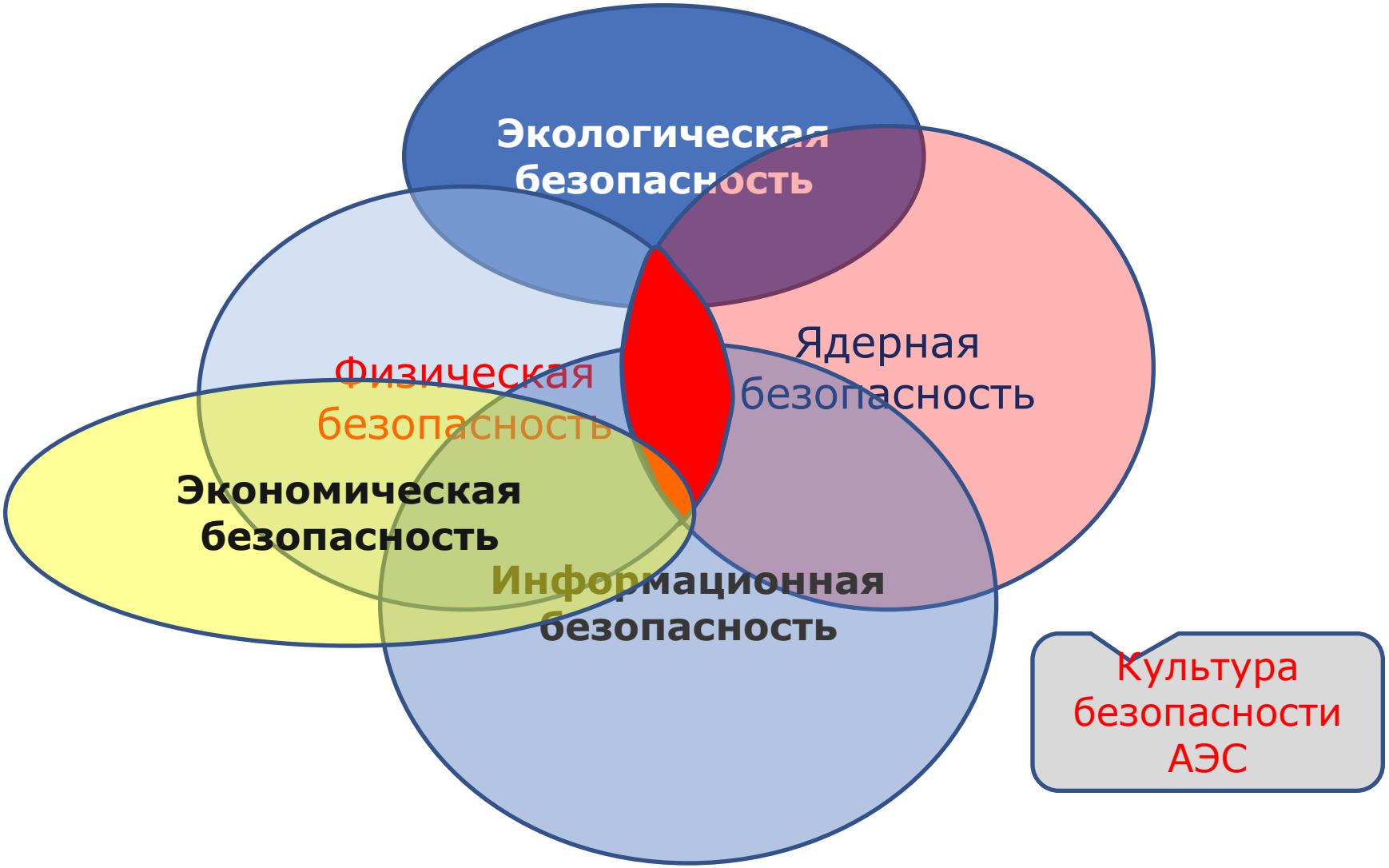
14.04.2013 15:05

В качестве превентивной меры против возможных кибератак единственный в Республике Корея оператор АЭС, Korea Hydro & Nuclear Power, отключил от Интернета свои внутренние компьютерные сети.

В Южной Корее сейчас действуют 23 атомных реактора, обеспечивающие до 35 % потребностей страны в электроэнергии.

Госкомпания также ограничила доступ в Интернет для своих систем управления атомными электростанциями, полностью отделив их от внутренних компьютерных сетей. С этой же целью в системах управления АЭС были опечатаны все USB-порты. Такие действия здесь считают наиболее надежным способом защиты станций от атак хакеров извне.
На днях официальный Сеул также заявил, что за недавними кибератаками, в результате которых пострадали серверы трех крупных банков и трех ведущих телеканалов страны, включая государственный KBS, стоит КНДР. Пхеньян отрицает свою причастность к атакам хакеров, которые вывели из строя 48 тысяч компьютеров.

Комплексная безопасность – культура безопасности



Иерархия Норм безопасности

В рамках своего мандата МАГАТЭ разработало логическую систему целей и принципов безопасности ядерных реакторов.

Основы Безопасности

- Излагают общие принципы защиты людей и охраны окружающей среды

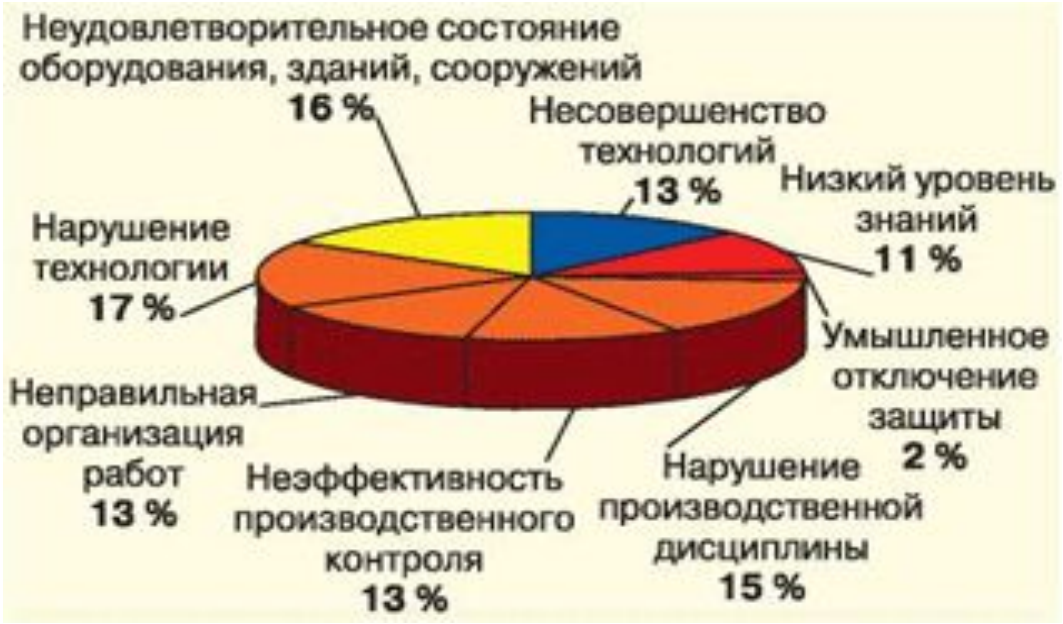
Требования Безопасности

- Устанавливают требования: что *должно* быть сделано для того, чтобы эти принципы применялись для достижения целей

Руководства по безопасности

- Представляют рекомендуемые методы, которые *следует* применять в обеспечение соблюдения этих требований

Статистика Ростехнадзора



Распределение причин нарушений на объектах повышенной опасности (красным цветом выделены причины нарушений, обусловленные человеческим фактором)

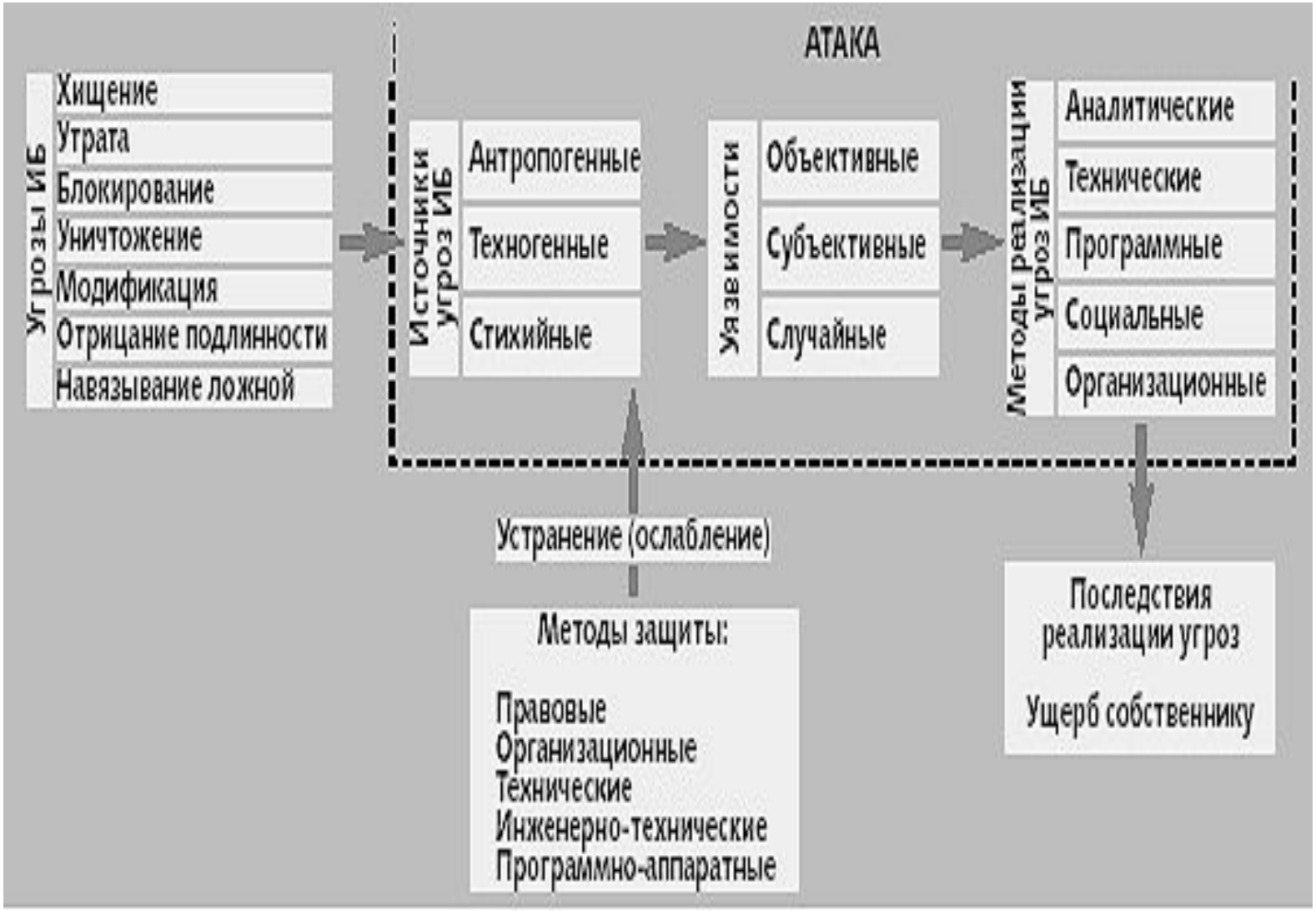
Система информационной безопасности

КОМПЛЕКСНОСТЬ

Для обеспечения безопасности используется комплекс мер, который включает в себя:

- технические меры
- правовые меры
- организационные меры
- физические меры

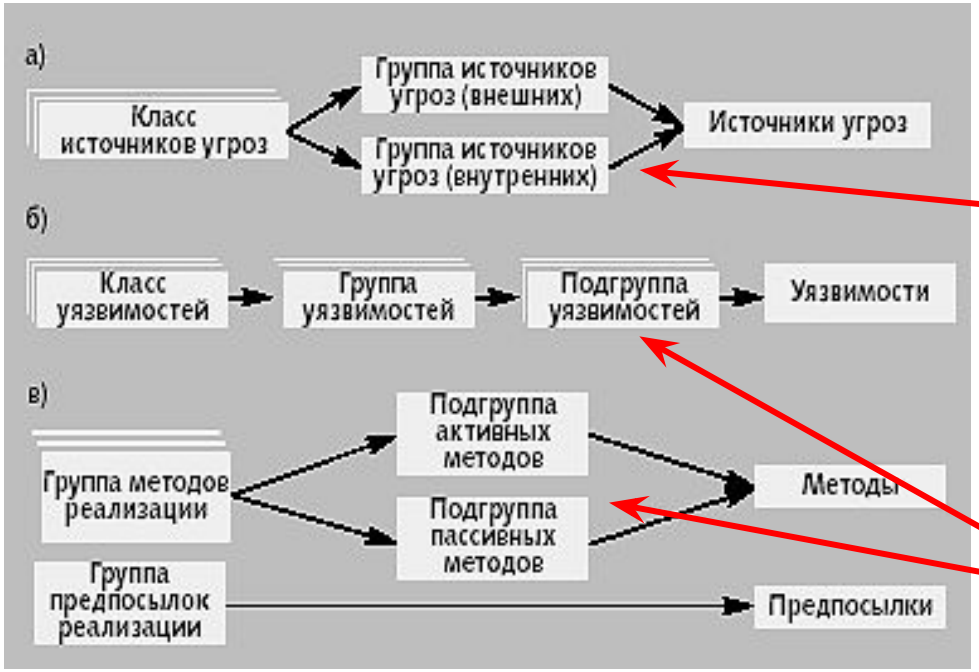
Аналитика информационной безопасности



Объекты анализа

- В ходе анализа необходимо убедиться, что все возможные источники угроз и уязвимости идентифицированы и сопоставлены друг с другом, а всем идентифицированным источникам угроз и уязвимостям сопоставлены методы реализации. При этом важно иметь возможность, при необходимости, не меняя самого методического инструментария, вводить новые виды источников угроз, методов реализации, уязвимостей, которые станут известны в результате развития знаний в этой области.
- Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, не зависящим от субъекта проявлений. Угроз не так уж и много.
- При обеспечении конфиденциальности информации это может быть хищение (копирование) информации и средств ее обработки, а также ее утрата (неумышленная потеря, утечка). При обеспечении целостности информации список угроз таков: модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации. При обеспечении доступности информации возможно ее блокирование, либо уничтожение самой информации и средств ее обработки.

Разработка мероприятий по обеспечению безопасности



Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (рис. 2а). Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис. 2б). Методы реализации можно разделить на группы по способам реализации (рис. 2в).

Классификация возможностей реализации угроз (атак), представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, т.е. как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Цели анализа

- установить приоритеты целей безопасности для субъекта отношений;
- определить перечень актуальных источников угроз;
- определить перечень актуальных уязвимостей;
- оценить взаимосвязь угроз, источников угроз и уязвимостей;
- определить перечень возможных атак на объект;
- описать возможные последствия реализации угроз.

- Под **утечкой информации** понимается бесконтрольный и неправомерный выход секретной или конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.
- Несанкционированный доступ к информации, обрабатываемой в автоматизированных системах, может быть **косвенным** (без физического доступа к элементам системы) и **прямым** (с физическим доступом), а также **активным** (с изменением элементов системы или информации) и **пассивным** (без изменения).
- Под **контролируемой зоной** понимают места, в пределах которых исключается бесконтрольное пребывание посторонних лиц. В связи с этим понятием принято различать угрозы, источник которых расположен вне контролируемой зоны, и угрозы, источник которых расположен в пределах контролируемой зоны.

К угрозам, источник которых расположен вне контролируемой зоны, можно отнести, например, такие:

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- дистанционная фото - и видеосъемка.

Примеры угроз, источник которых расположен в пределах контролируемой зоны:

- **хищение учтенных материальных носителей информации;**
- **хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);**
- **несанкционированное копирование информации;**
- **отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения, линий связи и т.д.);**
- **применение подслушивающих устройств.**

несанкционированного доступа к информации принято подразделять на следующие группы:

- - акустические (акустический контроль помещений, транспорта, непосредственно человека, контроль и прослушивание телефонных каналов связи);
- - визуально-оптические (наблюдение, фотографирование, видеозапись);
- - электромагнитные (перехват побочных электромагнитных излучений и наводок на соседние линии, цепи питания и заземления);
- - документально-предметные (хищение или несанкционированное копирование носителей информации);
- - аналитические (исследование открытых публикаций, разговоров, процессов деятельности, полезного продукта и отходов производства);
- - криптоаналитические (перехват и дешифрование засекреченных сообщений);
- - перехват компьютерной информации (перехват радиоизлучений компьютера, несанкционированное внедрение в базы данных);
- маскировка под законного пользователя системы.