

Министерство обороны Российской Федерации
ЧЕРНОМОРСКОЕ ВЫСШЕЕ ВОЕННО-МОРСКОЕ ОРДЕНА
КРАСНОЙ ЗВЕЗДЫ

УЧИЛИЩЕ ИМЕНИ П.С. НАХИМОВА

Факультет радиотехники и информационной безопасности

Кафедра электроники и информационной безопасности

Исследование проблем формирования системы показателей и критериев информационной безопасности Российской Федерации

Дипломная работа
студента 769 группы

Научный
руководитель

Рецензент

Голубевой
Кристины

к.т.н., доцент
Сапожникова А.В.

2018 г

- ▶ **Целью** дипломной работы является раскрытие и исследование проблемы формирования показателей и критериев информационной безопасности в Российской Федерации.
- ▶ **Объектом** исследования является модель нарушителя в информационной системе, комплекс средств и методов защиты информации.
- ▶ **Предметом** исследования являются теоретические и методические аспекты оценки эффективности защищенности информации.
- ▶ **Актуальность** выбранной темы обусловлена тем, что при принятии решения по оценке информационной безопасности для любого предприятия важно достижение максимального показателя защищенности от угроз. Соизмерение затрат и результатов позволяет предупредить возможные убытки при внедрении проекта, оценить эффективность метода защиты информационной системы с учетом имеющихся рисков.
- ▶ Дипломная работа состоит из введения, трех разделов, заключения и списка литературы.

Введение

Государственная информационная безопасность представляет собою состояние сохранности всех информационных ресурсов государства, а также защищенность всех законных прав общества и личности в информационной сфере.



Построение системы защиты информации по ФСТЭК России

- ▶ Система защиты информации по ФСТЭК России строится на 3 основных ступенях (и соответствующих проверках):
- ▶ **Организационные меры.** Проверка достаточности политик безопасности, принятых в организации, для нейтрализации возможных угроз безопасности.
- ▶ **Защита от утечки по техническим каналам.** Оценка соответствия искомого показателя нормированным значениям.
- ▶ **Защита от несанкционированного доступа и несанкционированного воздействия.** Проверка соответствия состава внедренных мер и средств защиты информации и их настроек существующим требованиям (например, нормативно-правовые акты федеральных органов исполнительной власти, руководящие и методические документы, российские и международные стандарты, стандарты организации и пр.).

Понятие критерия и показателя безопасности

- ▶ Для всех мероприятий, которые определяют защищенность системы от НСД и ТКУИ существуют такие понятия как «показатель» и «критерий» ИБ. Расшифруем эти понятия:
- ▶ Показатель информационной безопасности - это мера или характеристика для оценки информационной безопасности.
- ▶ Критерий обеспечения ИБ организации - показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.

Нормативно-правовая база и законодательство в сфере информационной безопасности

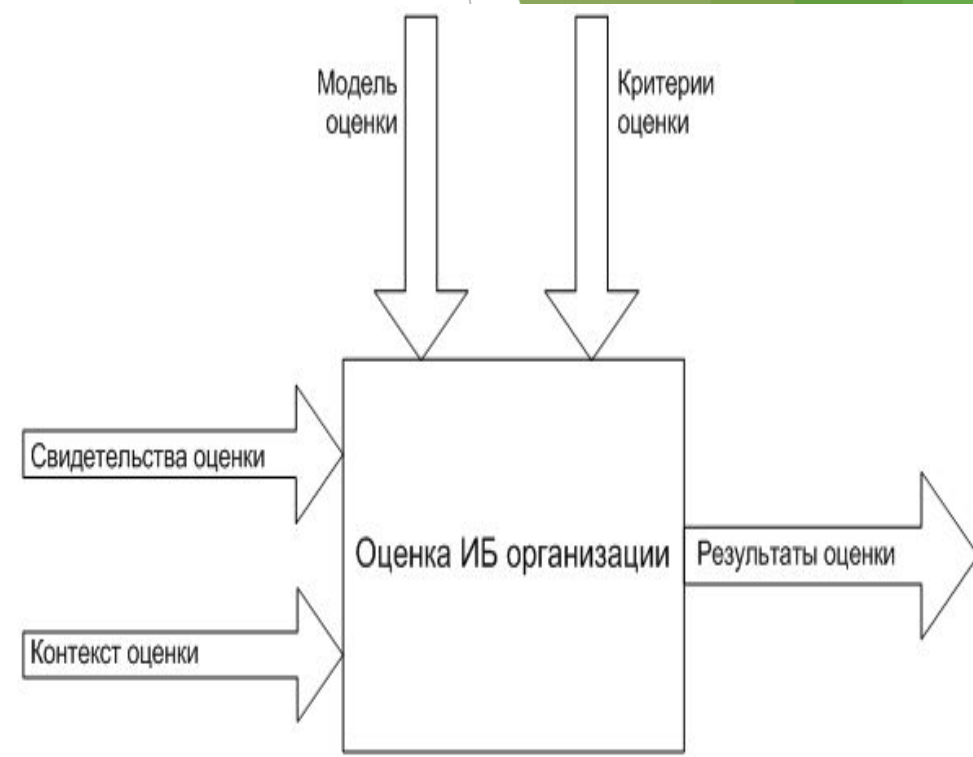


Основные принципы обеспечения безопасности

- ▶ Согласно Федеральному закону от 28 декабря 2010 г. N 390-ФЗ "О безопасности", основными принципами обеспечения безопасности являются:
- ▶ 1) соблюдение и защита прав и свобод человека и гражданина;
- ▶ 2) законность;
- ▶ 3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
- ▶ 4) приоритет предупредительных мер в целях обеспечения безопасности;
- ▶ 5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Процесс оценки ИБ

- ▶ В общем виде процесс проведения оценки ИБ (рис. 2) представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки, - необходимыми для реализации процесса оценки.
- ▶ Оценка ИБ заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения ИБ, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических элементов (факторов) объекта оценки.
- ▶
- ▶ Процесс оценки ИБ включает следующие элементы проведения оценки:
 - ▶ - контекст оценки, который определяет входные данные: цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли;
 - ▶ - критерии оценки;
 - ▶ - модель оценки;
 - ▶ - мероприятия процесса оценки: сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов объекта оценки;
 - ▶ - выходные данные оценки.



Свойства дефектов качества информационных систем определяются такими факторами:

количество разработчиков информационных систем

условия обеспечения процесса разработки

характеристики специальных средств и элементов

уровень агрессивности и сложности внешней среды

сложность выполняемых при помощи информационных систем процедур

Существует специальная модель классификации критериев качества информационных систем:



Стандарты оценки ИС

- ▶ Стандарты оценки ИС - это совокупность всех свойств, в которых обусловлена возможность ее применения для удовлетворения потребностей в соответствии с ее назначением. Именно количественные характеристики каждого такого свойства определяют основные виды показателей.
- ▶ Что касается модели качества программного обеспечения, то на сегодняшний день наибольшее распространение получила многоуровневая модель. Она представлена стандартом ISO 9126. Сначала она выделяет шесть основных характеристик качеств программного обеспечения, а далее их атрибуты, которые включают в себя соответствующие метрики для дальнейшей оценки всей ИС.

**Основные виды
показателей
качества
информационных
систем**

Безопасность

обеспечение максимальной конфиденциальности, а также целостности всей имеющейся информации – защита информации от любого несанкционированного доступа

секретность информации

используемые программно-технические средства

прогнозируемая сумма ущерба

порядок доступа и работы в сети

Достоверность

набор свойств, который определяет безошибочность преобразований информации

единичные

корректировки ИС

комплексные

Надежность

набор свойств, сохраняющих время всех параметров, которые необходимы для выполнения определенных функций

безотказность

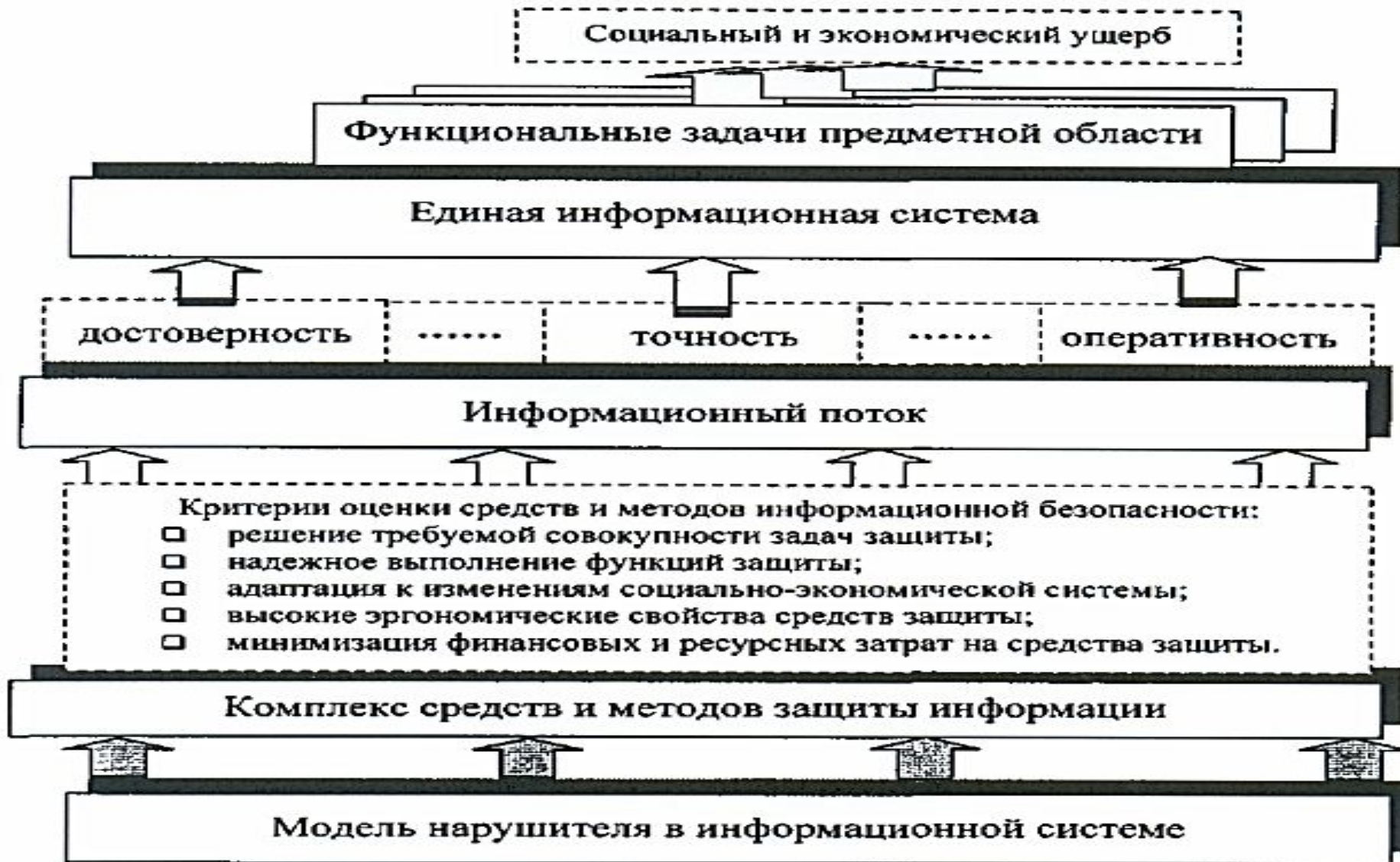
ремонтпригодность

долговечность

Локальные показатели эффективности ИС

- ▶ Эффективность системы является сложным, интегральным свойством, зависящим от ряда простых свойств, влияющих на оптимальность функционирования системы, таких как:
- ▶ действенности системы, то есть степени удовлетворения системой своего предназначения, (прагматическая эффективность, pragmatos [греч.] — действие);
- ▶ технического совершенства системы (технической эффективности);
- ▶ простоты и технологичности разработки и создания системы (технологической эффективности);
- ▶ удобства использования и обслуживания системы (эксплуатационной эффективности) и ряда других характеристик.

СОЗДАНИЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИ НАРУШИТЕЛЯ



Разработка методик и алгоритмов оценки показателей и критериев ИБ