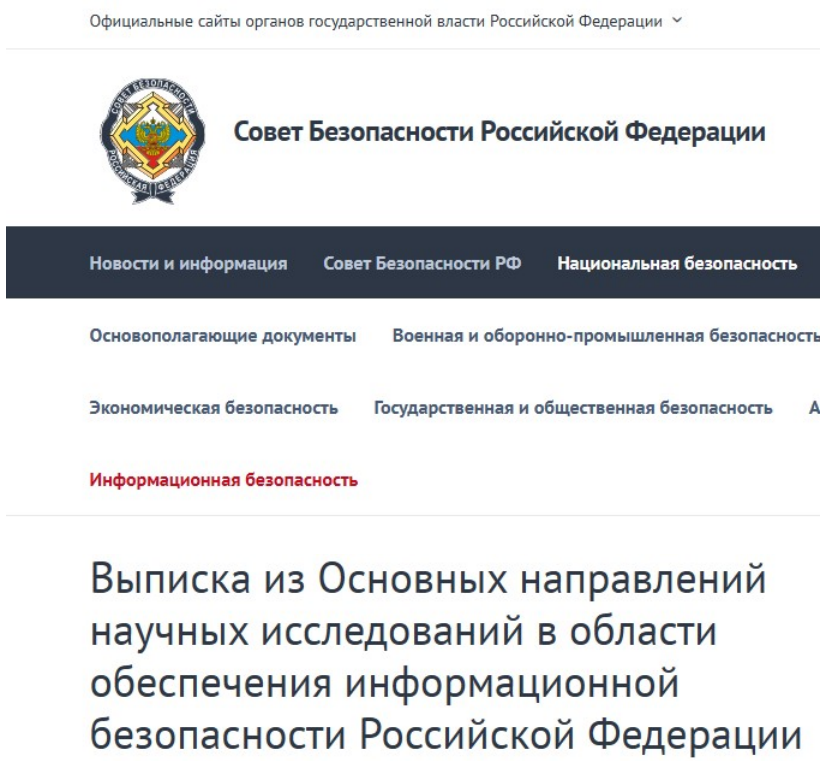
Оценка информационной безопасности

Бизянов Е.Е.

Основные федеральные органы, обеспечивающие ИБ

- ФСБ
- Министерство обороны
- Министерство внутренних дел
- Минкомсвязь
- ФСТЭК
- Государственная Дума
- И др.

http://www.scrf.gov.ru/security/information/document155/



1. Общенаучные проблемы обеспечения информационной безопасности Российской Федерации:

……

1.1.6. Проблемы оценки информационной безопасности личности, общества и государства.

Государственные стандарты Российской Федерации (28)

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»

ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»

ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»

ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»

ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»

ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»

ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки»

ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»

ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»

ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»

ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»

ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»

ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2. Порядок оценки угроз безопасности информации

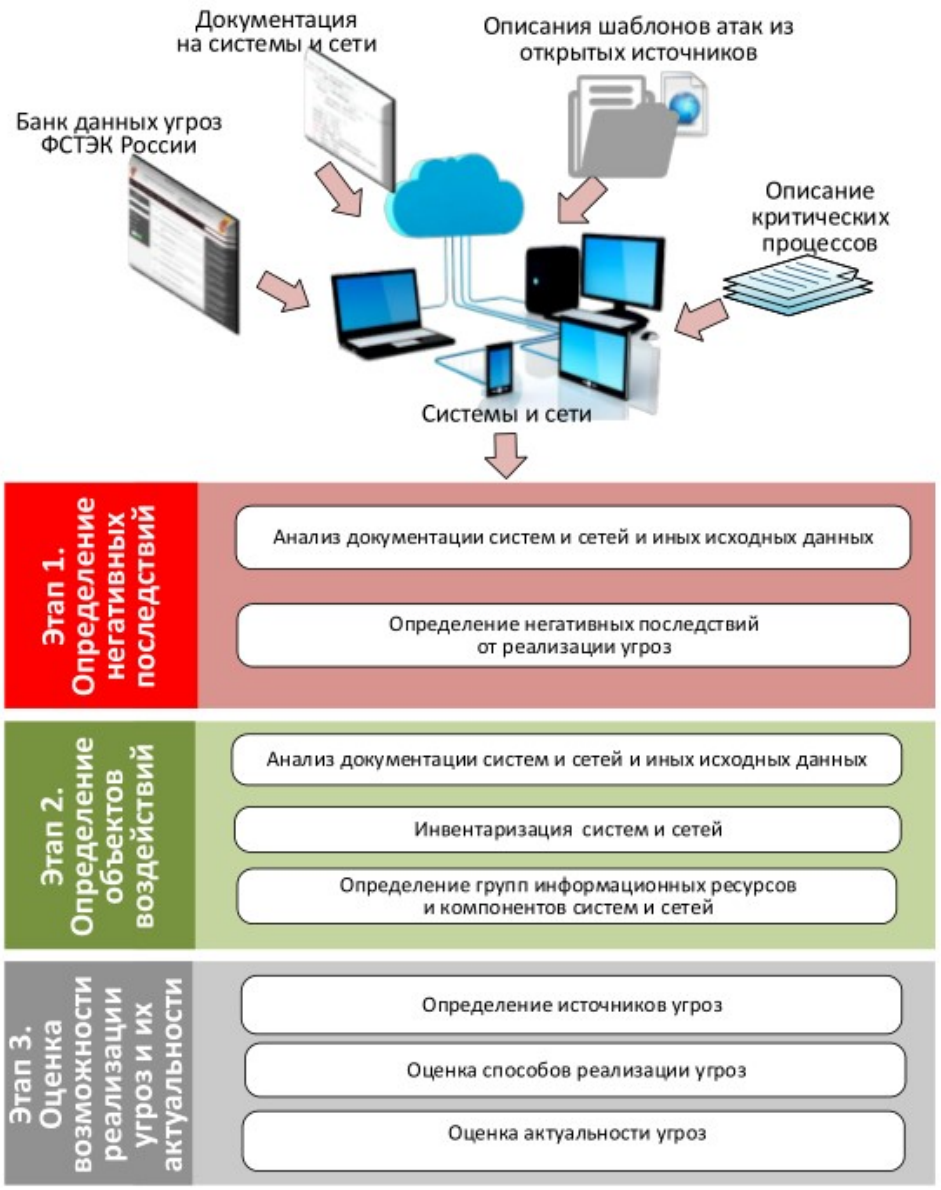


Рисунок 2. Общая схема проведения оценки угроз безопасности информации

3. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

4. Определение возможных объектов воздействия угроз безопасности информации

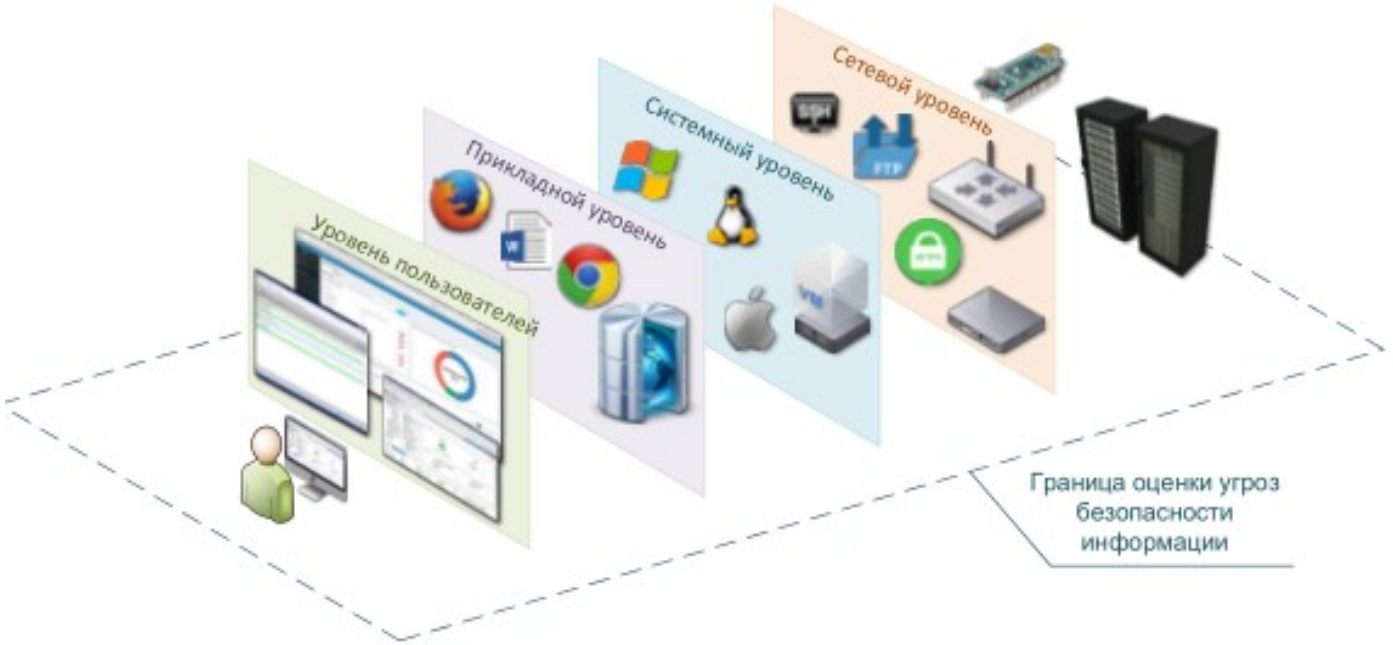


Рисунок 3. Уровни архитектуры систем и сетей, на которых определяются объекты воздействия

5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

5.1 Определение источников угроз безопасности информации

5.2 Оценка способов реализации (возникновения) угроз

безопасности информации

5.3 Оценка актуальности угроз безопасности информации

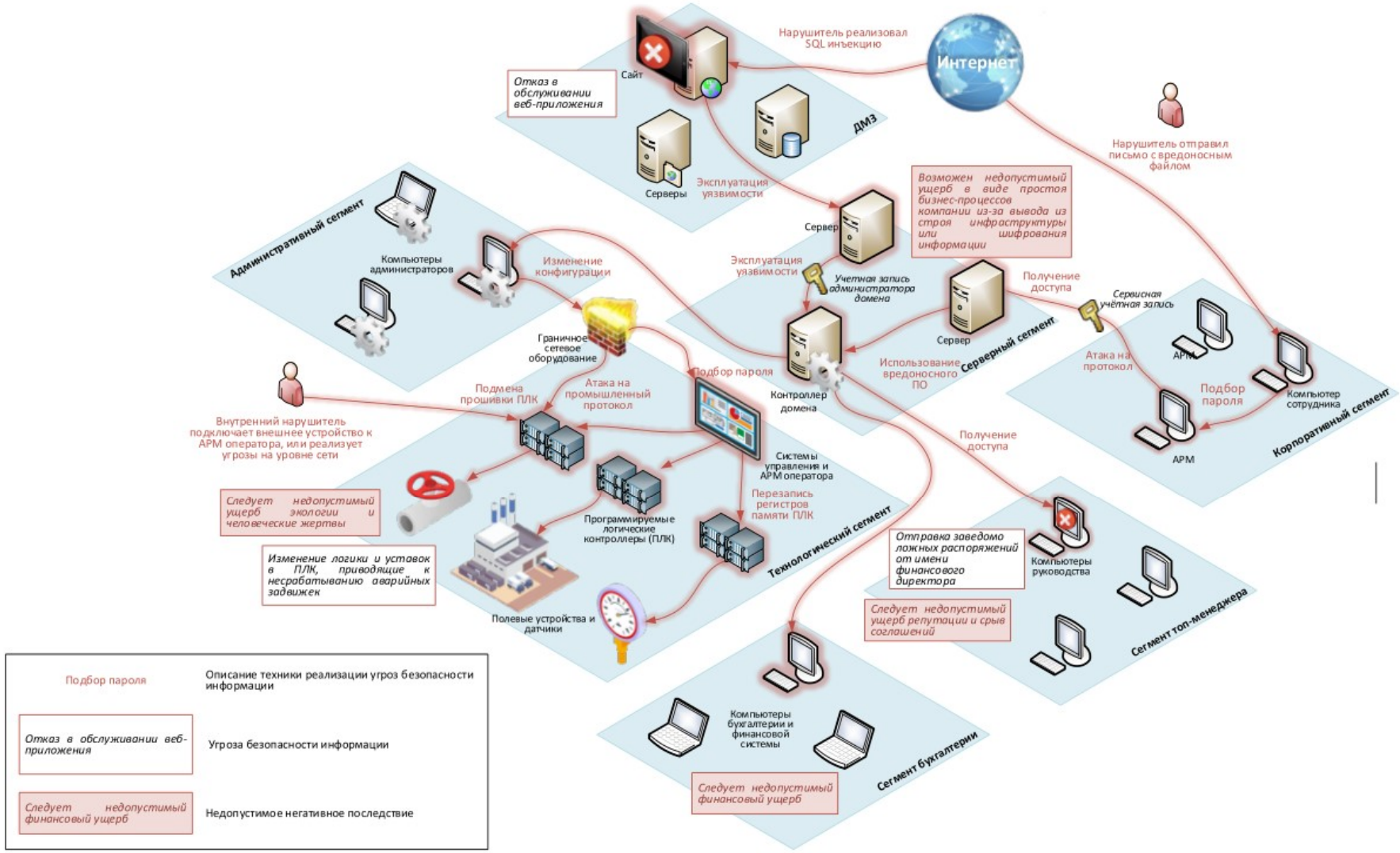


Рисунок 8. Пример сценариев реализации угроз безопасности информации

11 приложений:

1. Термины и определения
2. Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации

Пример таблицы результатов оценки параметров

Эксперты	Значение оцениваемого параметра (раунд 1)	Значение оцениваемого параметра (раунд 2)
Эксперт 1		
Эксперт 2		
Эксперт n		
Итоговое значение		

Вычисляется средняя оценка

3. Рекомендуемая структура модели угроз безопасности информации

1. Общие положения
2. Описание систем и сетей и их характеристика как объектов защиты
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации (возникновения) угроз безопасности информации
7. Актуальные угрозы безопасности информации

4. Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации

Таблица 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Угроза жизни или здоровью. Унижение достоинства личности. Нарушение свободы, личной неприкосновенности. Нарушение неприкосновенности частной жизни. Нарушение личной, семейной тайны, утрата чести и доброго имени. Нарушение тайны переписки, телефонных переговоров, иных сообщений. Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. «Травля» гражданина в сети «Интернет». Разглашение персональных данных граждан
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Нарушение законодательства Российской Федерации. Потеря (хищение) денежных средств. Недополучение ожидаемой (прогнозируемой) прибыли.

5. Примеры определения объектов воздействия и видов воздействия на них

Таблица 5.1

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Утечка идентификационной информации граждан с АРМ пользователя
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы
Хищение денежных средств со счета организации (У2)	Банк-клиент	Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения
	[illegible]	[illegible]

6. Возможные цели реализации угроз безопасности информации нарушителями

Таблица 6.1

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса
2	Террористические, экстремистские группировки	Внешний	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
4	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)

7. Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации (для государственной информационной системы)

Таблица 7.1

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Специальные службы иностранных государств	-	-	+ (дискредитация или дестабилизация деятельности органа государственной власти*)	У3** (нарушение функционирования государственного органа, дискредитация деятельности органа государственной власти)
Террористические, экстремистские группировки	-	-	+ (дестабилизация деятельности органов государственной власти, организаций)	У3 (отсутствие доступа к социально значимым государственным услугам)

8. Уровни возможностей нарушителей по реализации угроз безопасности информации

Таблица 8.1

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими	Преступные группы (два лица и более, действующие по единому плану) Конкурирующие организации Поставщики вычислительных услуг,

9. Примеры результата определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности (для государственной информационной системы)

Таблица 9.1

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности персональных данных граждан; нарушение личной, семейной тайны, утрата чести и доброго имени; финансовый, иной материальный ущерб физических лиц	Преступные группы (криминальные структуры)	Внешний Внутренний***	Н3
		Отдельные физические лица (хакеры)	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
2	У2: невозможность заключения договоров, соглашений;	Преступные группы (криминальные структуры)	Внешний	Н3
		Отдельные	Внутренний	Н2

10. Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности (для государственной информационной системы)

Таблица 10.1

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Специальные службы иностранных государств (Н4)	Внешний	База данных информационной системы, содержащая идентификационную информацию граждан: несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным; утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных	Веб-интерфейс удаленного администрирования базы данных информационной системы	Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования
				Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных: перехват (нарушение конфиденциальности) защищаемой информации,	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка программных закладок в телекоммуникационное оборудование

11. Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

Таблица 11.1

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера

Проблема использования экспертных оценок

Орлов А.И. Экспертные оценки. – Журнал «Заводская лаборатория». 1996. Т.62. No.1. С.54-60

ДОГМА СОГЛАСОВАННОСТИ

Считается, что решение может быть принято лишь на основе согласованных мнений экспертов. Поэтому **исключают** из экспертной группы тех, чье мнение отличается от мнения большинства. При этом отсеиваются как **неквалифицированные** лица, попавшие в состав экспертной комиссии по недоразумению или по соображениям, не имеющим отношения к их профессиональному уровню, так и наиболее **оригинальные** мыслители, глубже проникшие в проблему, чем большинство.

Проблема использования экспертных оценок

ДОГМА ОДНОМЕРНОСТИ

Распространен довольно примитивный подход так называемой «квалиметрии», согласно которому объект всегда можно оценить одним числом. Оценивать человека одним числом приходило в голову лишь на невольничьих рынках. Вряд ли даже самые рьяные квалиметристы рассматривают книгу или картину как эквивалент её "рыночной стоимости".

ОСНОВНЫЕ СТАДИИ ЭКСПЕРТНОГО ОПРОСА

1) формулировка Лицом, Принимающим Решения, цели экспертного опроса;

2) подбор ЛПР основного состава Рабочей группы;

3) разработка РГ и утверждение у ЛПР технического задания на проведение экспертного опроса;

4) разработка РГ подробного сценария проведения сбора и анализа экспертных мнений (оценок), включая как конкретный вид экспертной информации (слова, условные градации, числа, ранжировки, разбиения или иные виды объектов нечисловой природы) и конкретные методы анализа этой информации (вычисление медианы Кемени, статистический анализ люсианов и иные методы статистики объектов нечисловой природы и других разделов прикладной статистики);

5) подбор экспертов в соответствии с их компетентностью;

6) формирование экспертной комиссии (целесообразно заключение договоров с экспертами об условиях их работы и ее оплаты, утверждение ЛПР состава экспертной комиссии);

7) проведение сбора экспертной информации;

8) анализ экспертной информации;

9) при наличии нескольких туров - повторение двух предыдущих этапов;

10) интерпретация полученных результатов и подготовка заключения для ЛПР;

11) официальное окончание деятельности РГ.

ПОДБОР ЭКСПЕРТОВ

Проблема подбора экспертов является одной из наиболее сложных.

Очевидно, в качестве экспертов необходимо использовать **тех людей, чьи суждения наиболее помогут принятию адекватного решения**. Но как выделить, найти, подобрать таких людей? Надо прямо сказать, что нет методов подбора экспертов, наверняка обеспечивающих успех экспертизы.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА ЭКСПЕРТНЫХ ОЦЕНОК

Можно выделить основные широко используемые в настоящее время методы математической обработки экспертных оценок - это проверка **согласованности** мнений экспертов (или классификация экспертов, если нет согласованности) и **усреднение** мнений экспертов внутри согласованной группы.

Поскольку ответы экспертов во многих процедурах экспертного опроса - не числа, а такие объекты нечисловой природы, как градации качественных признаков, ранжировки, разбиения, результаты парных сравнений, нечеткие предпочтения и т.д., то для их анализа оказываются полезными методы статистики объектов нечисловой природы

Почему ответы экспертов носят нечисловой характер? Наиболее общий ответ состоит в том, что люди не мыслят числами. В мышлении человека используются образы, слова, но не числа. Поэтому требовать от эксперта ответа в форме числа - значит насиловать его разум.

Эксперт может сравнить два объекта, дать им оценки типа "хороший", "приемлемый", "плохой", упорядочить несколько объектов по привлекательности, но обычно не может сказать, во сколько раз или на сколько один объект лучше другого. Другими словами, ответы эксперта обычно измерены в порядковой шкале, являются ранжировками, результатами парных сравнений и другими объектами нечисловой природы, но не числами.

ИНТЕРВАЛЬНЫЕ ЭКСПЕРТНЫЕ ОЦЕНКИ

Перспективным является использование интервальных экспертных оценок: эксперт называет не число, а интервал в качестве оценки рассматриваемого параметра. Такие процедуры удачно сочетают в себе количественный и качественный подходы в экспертных оценках.

Показатели:

1. производительность информации
2. коэффициент информационной вооруженности
3. коэффициент защищенности информации
4. оценка программно-технической защищенности информации
5. оценка информационной надежности персонала
6. оценка информации, предоставляемой лицам, принимающим решения, информационной службой предприятия.
7. Для проведения оценки в качестве критериев эффективности системы организации информационной безопасности используются, например, показатели совокупной стоимости владения (Total Cost of Ownership – TCO).

В процессе оценки эффективности комплексной системы защиты информации, они выделяют три подхода: классический, официальный, экспериментальный.

Под классическим подходом к оценке эффективности понимается использование критериев эффективности, значения которых получаются путем моделирования или определяются по характеристикам реальной информационной системы.

Основные проблемы оценки ИБ

1. Разнообразие архитектур защищаемых информационных систем
2. Субъективность экспертных оценок
3. Возможность – вероятность
4. Предлагаемые методы и модели производят оценку или в виде вероятностей возникновения угроз, или экспертно.
5. Нарушители ИБ совершенствуются также быстро, как и её защитники. Чаще первые идут впереди вторых.

Перспективы – ИИ и пр.

1. Нечеткая логика и нечеткая математика
2. Модель Байеса
3. Машинное обучение
4. Data Mining & Big Data

Отдельно отметим, что нужны *объективные* оценки ИБ, которые можно представить в числовой форме – как «обычные» числа или нечёткие числа.