Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:

Руководитель программы аспирантуры

_____ А.Н. Привалов
(подпись)

«18» марта 2026 г.

Рабочая программа дисциплины
АНАЛИЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы и форма обучения:	3 года

Шуя

1. Цели освоения дисциплины

Целью учебной дисциплины является содействие аспирантам в приобретении знаний, умений и навыков в области проведения анализа безопасности компьютерных систем, необходимых в процессе проведения практических работ в рамках диссертационного исследования. В рамках данного курса предполагается изучение основ аудита безопасности компьютерных систем и технологии технического аудита для определения защищённости компьютерных систем в организациях.

2. Место дисциплины в структуре ОП

Дисциплина «Анализ безопасности компьютерных систем» является дисциплиной по выбору блока дисциплин «Дисциплины (модули) по выбору 2 (ДВ.2)».

Успешное освоение данной дисциплины будет способствовать готовности аспирантов к подготовке публикаций и (или) заявок на патенты на изобретения, полезные модели, свидетельства о государственной регистрации программ для электронных вычислительных машин, баз данных, топологий интегральных микросхем, подготовке к прохождению промежуточной аттестации по этапам выполнения научного исследования, итоговой аттестации.

Для освоения данной дисциплины обучающийся должен:

Знать:

−основные нормативно-правовые документы и стандарты в области информационной безопасности;

Уметь:

−работать с документацией, описывающей построенную структуру безопасности информационной системы;

Владеть:

−современной терминологией в области информационной безопасности.

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

Знать:

– основные угрозы нарушения безопасности компьютерных систем и методы их реализации;
– архитектуры защищенных компьютерных систем;
– современные механизмы, технологии и средства обеспечения безопасности в сетях;
– типовые схемы подключения сетевого оборудования и средств защиты;
– методологии анализа защищенности;
– методики оценки защищенности компьютерных систем на основе данных анализа.

Уметь:

– определять потенциально уязвимые места в компьютерной системе;
– выбирать и обосновывать методы и технологии защиты в компьютерных системах;
– настраивать механизмы защиты сетевой инфраструктуры;
– анализировать защищенность компьютерных систем;
– оценивать риски, связанные с проведением анализа, и мер по их минимизации;
– обнаруживать нарушения безопасности в компьютерных системах и проводить их анализ.

Иметь опыт:

– проектирования защищенных компьютерных систем;
– анализа нарушений безопасности;

– проведения оценочных работ по соответствию защищаемых объектов информации и компьютерных систем действующей нормативно-правовой документации;

– использования инструментальных средств анализа защищенности компьютерных систем.

4. Объем и содержание дисциплины

Объем дисциплины составляет 2 зачетных единицы (36 академических часов)

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

№	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в акад. часах, по очной форме обучения)			Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинарского типа	Самостоятельная работа обучающихся	
1.	Общие сведения о безопасности компьютерных систем, проведении ее анализа	3	2	2 практические	4	Практические задания
2.	Содержание работ при аудите безопасности информационных систем	3	2	2 практические	4	Практические задания
3.	Методология проведения аудита информационной безопасности	3	2	2 практические	4	Практические задания
4.	Отчёт об аудите безопасности АИС	3	2	2 практические	4	Практические задания
5.	Унифицированные программные средства поддержки аудита информационной безопасности	3	2	2 практические	4	Реферат
6.	Корпоративная политика информационной безопасности	3	2	2 практические	4	Практические задания
7.	Инструментальные средства аудита ИБ	3	2	2 практические	4	Практические задания
8.	Изучение практического опыта технического аудита безопасности АИС предприятий	3	2	2 практические	4	Практические задания
9.	Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины	3	2	2 практические	4	Практические задания
10.	Итого за семестр:		18	18	36	Зачет с оценкой

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Тема 1 – Общие сведения о безопасности компьютерных систем, проведении ее анализа

Понятие многоуровневой защиты. Основные механизмы обеспечения сетевой безопасности. Модель многоуровневой защищенной корпоративной сети. Защита от атак в ЛВС. Основные элементы архитектуры межсетевых экранов. Технология фильтрации пакетов межсетевых экранов. Технология контроля состояний межсетевых экранов. Технология унифицированного межсетевого экранирования. Основные схемы подключения межсетевых экранов. Технология PVLAN. Сущность аудита информационной безопасности. Внешний и внутренний аудит. Постановка проблемы аудита безопасности. Общая характеристика критериев аудита информационной безопасности. Основные нормативные документы, используемые при организации аудита. Национальные и отраслевые стандарты безопасности компьютерных систем. Термины и определения. Необходимость и актуальность аудита безопасности. Особенности автоматизированных информационных систем как объектов аудита ИБ. Основные характеристики информационного и организационно-методического обеспечения безопасности функционирования организаций.

Тема 2 – Содержание работ при аудите безопасности информационных систем

Цели и виды аудита информационной безопасности. Основные этапы работ по проведению аудита безопасности. Этапы проведения аудита. Стадии аудита: планирование; моделирование; тестирование; анализ; разработка предложений; документирование. Принципы и формы аудита ИБ. Формы обследования (аудита): первоначальное обследование (первичный аудит); предпроектное обследование (технический аудит); аттестация объекта; сюрвей; плановое обследование (контрольный аудит). Техника аудита. Ведение записей. Основные и дополнительные задачи внутреннего аудита безопасности информационных систем. Этапы и содержание работ по проведению аудита ИБ. Инициирование процедуры аудита . Подготовка к аудиту и общая схема его проведения. Технология сбора информации аудита. Планирование и осуществление процедуры аудита. Методика подготовки аудитора. Дополнительные задачи, стоящие перед внутренним аудитором. Перечень и состав документов. Сбор свидетельств. Формулирование несоответствий.

Тема 3 – Методология проведения аудита информационной безопасности

Основные подходы к анализу данных. Задачи анализа и управления рисками информационной безопасности. Интервью с сотрудниками организации с использованием заранее подготовленных и стандартизованных опросных листов. Оценка состояния информационной безопасности на соответствие стандартам. Обязанности и правила этики аудитора. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы и средства анализа защищенности. Документирование системы и анализ рисков с использованием специализированного программного инструментария и шаблонов отчетов. Анализ организационно-распорядительной документации по обеспечению режима информационной безопасности. Оценка процессов обеспечения информационной безопасности в организации, квалификации сотрудников, знания ими своих должностных обязанностей и степени их осведомленности в вопросах информационной безопасности. Оценка достаточности физических механизмов безопасности. Обоснование требований по результатам оценки рисков.

Тема 4 – Отчёт об аудите безопасности автоматизированных информационных систем

Методика подготовки отчётных документов после проведенного аудита, структура и содержание отчёта. Рекомендации организации, предприятию по результатам аудита. Оформление общего отчета. Представление о степени профессиональной квалификации аудитора. Законодательная и нормативная база аудита ИБ. Классификация уязвимостей АИС.

Тема 5 – Методическое обеспечение аудита информационной безопасности

Методы и подходы к управлению рисками информационной безопасности. Выявление и оценка угроз, уязвимостей, возможного ущерба. Выбор стратегий управления рисками. Обзор современных программных средств анализа и управления рисками информационной безопасности. Основные классификационные признаки компьютерных вирусов. Технологии обнаружения заражения вирусами. Документация системы управления информационной безопасностью. Выбор стратегии управления рисками ИБ. Обоснование необходимых мер безопасности.

Тема 6 – Корпоративная политика информационной безопасности

Корпоративная политика безопасности; организационно-распорядительные документы организации. Формирование политики информационной безопасности организации. Определение требуемого уровня ИБ. Остаточные риски. Ядро системы комплексной защиты информации. Ресурсы комплексной системы защиты информации. Интегральные критерии информационной безопасности организации. Методы сбора исходных данных. Сбор исходной информации для проведения аудита, такие как: общие исходные данные, исходные данные об обрабатываемой информации, исходные данные о системе обеспечения безопасности информации исходные данные о персонале, сбор дополнительных исходных данных.

Тема 7. Инструментальные средства аудита информационной безопасности

Методы и инструментальные средства проведения активного аудита ИБ. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности, мониторинг событий безопасности. Классификация и архитектура сканеров безопасности. Схемы подключения сканеров безопасности. Основные этапы работы сканеров безопасности. Особенности проведения сканирования корпоративных вычислительных сетей. Внедрение сканеров безопасности в корпоративной сети. Подключение сетевых средств защиты с высокой доступностью. Общие требования и особенности. Методы сбора информации о сети. Методы идентификация устройств в сети и их реализация в сканерах безопасности. Пассивный анализ информационных потоков. Методы идентификация открытых портов и их реализация в сканерах безопасности. Методы идентификация служб и приложений узла и их реализация в сканерах безопасности.

Тема 8 – Изучение практического опыта технического аудита безопасности АИС предприятий

Анализ опыта и рекомендации по планированию: инициирование процедуры аудита, цель планирования, объект обследования, порядок планирования аудита, анализ значимости информационных ресурсов, анализ процесса обработки информации, отчетные материалы, условия соблюдения конфиденциальности.

Анализ опыта и рекомендации по моделированию: цель моделирования, методы обследования на этапе моделирования, порядок проведения моделирования, отчетные материалы.

Анализ опыта и рекомендации по тестированию: цель, методы и порядок проведения тестирования, проверка реальных условий размещения и использования оборудования, тестовые испытания функций защиты от НСД и защиты от утечки по техническим каналам, отчетные материалы.

Анализ опыта и рекомендации по анализу и документированию результатов: цель и методы обследования на этапе анализа, анализ организационно-распорядительных документов, выполнения организационно-технических требований, деятельности персонала (сотрудников), отчетные материалы, рекомендации по документированию результатов: цель документирования.

Тема 9 – Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины

5. Образовательные технологии

В программе данного курса предусмотрено использование в учебном процессе активных форм проведения занятий и организации самостоятельной работы. В учебном процессе

предусмотрено использование технологий проблемного обучения, а также предметно-ориентированных технологий обучения, таких как: технология экспертной оценки состояния информационной безопасности; технология дистанционного анализа уязвимостей АИС; технология математического моделирования конфликтных ситуаций; технология процессного анализа состояния ИБ.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, мультимедиа технологии, облачные технологии, технологии визуализации (инфографика, дашборды).

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся по дисциплине осуществляется в следующих формах:

- повторение материала с использованием конспектов лекций;
- изучение и анализ предложенных электронных образовательных ресурсов, содержащих информацию по анализу безопасности компьютерных систем;
- выполнение заданий, из которых складывается портфолио студента, включающее обязательные и дополнительные (определяемые студентами совместно с преподавателем) материалы.

Задания и результаты их выполнения составляют часть информационного ресурса кафедры математики, информатики и методики обучения и хранятся на сервере кафедры, доступ к ним обеспечен с компьютеров в компьютерном классе.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется при помощи электронной информационно-образовательной среды Шуйского филиала ИвГУ.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация по дисциплине (зачет с оценкой) проводится с использованием рейтинговой оценки.

Промежуточная аттестация аспирантов предполагает зачет с оценкой в форме выполнения тестового задания, примерный вариант которого представлен в Приложении 2.

Критерии оценки:

- оценка «отлично» выставляется аспиранту, если аспирант выполнил тестового задание на 85 или более процентов;
- оценка «хорошо» выставляется аспиранту, если аспирант выполнил тестового задание на 71 или более процентов;
- оценка «удовлетворительно» выставляется аспиранту, если аспирант выполнил тестового задание на 61 или более процентов;
- оценка «неудовлетворительно» выставляется аспиранту, если аспирант выполнил тестовое задание на менее чем 61 процент;

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 100 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1277-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

2. Веселов, Г. Е. Менеджмент риска информационной безопасности : учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 109 с. : схем., табл. - Библиогр.: с.85-86 - ISBN 978-5-9275-2327-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493331

3. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

Дополнительная литература:

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

2. Артемов, А. В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605

3. Галатенко, В. А. Основы информационной безопасности : курс лекций : учебное пособие / В. А. Галатенко ; Интернет университет информационных технологий ; под ред. В. Б. Бетелина. - 2-е изд. ; испр. - Москва : Интернет-Университет Информационных Технологий, 2006. - 208 с. - URL: http://biblioclub.ru/index.php?page=book&id=233063

4. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. : схем., табл., ил. - Библиогр.: с. 213. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480636

5. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

6. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

7. Информационная безопасность : учебно-методические материалы для проведения практических занятий / Министерство образования и науки РФ; ГОУ ВПО "Шуйский государственный педагогический университет" ; авт.-сост. А. А. Михайлов, Г. Д. Хубулов. - Шуя : Изд-во ГОУ ВПО "ШГПУ", 2010. - 56 с.

8. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - М. : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774

9. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204

10. Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с. – Режим доступа: https://rucont.ru/efd/304393

Ресурсы информационно-телекоммуникационной сети «Интернет»:
Профессиональные базы данных и информационно-справочные системы:
ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
Национальный цифровой ресурс Руконт - https://rucont.ru/default.aspx
Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru
Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

– для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

– для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: электронные пособия (презентации), аудио-визуальные пособия (видеоматериалы), печатные пособия (таблицы, схемы)).

Автор(ы) рабочей программы дисциплины: профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор Привалов А. Н.

Программа рассмотрена и утверждена на заседании кафедры математики, информатики и методики обучения «02» марта 2022 г., протокол № 8

Программа обновлена
протокол заседания кафедры № 8 от «22» марта 2023 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 7 от «9» февраля 2024 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «20» марта 2025 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «18» марта 2026 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

Приложение 1
к рабочей программе дисциплины

Методические указания
для обучающихся по освоению дисциплины
АНАЛИЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы:	3 года

Шуя

1. Методические указания к проработке лекционного материала по дисциплине

Общий план лекций включает следующие составные элементы:

Название этапа	**Содержание**	**Время, мин.**
Вступительная часть	Приветствие. Контроль посещаемости. Постановка темы, цели, основных задач.	4-7
Актуальность и основные понятия	Формулирование проблемы; основные понятия и суть изучаемого вопроса.	8-10
Основная часть	Представление материала лекции в соответствии с программой	60-65
Закрепление полученной информации	Вопрос-ответ, фронтальный опрос, разбор ошибок, допущенных при ответах	5-8
Подведение итогов	Сопоставление результатов лекции с установленной целью и намеченными задачами.	3

В рамках проведения занятий по дисциплине предполагается чтение следующих лекций:

Лекция 1. Общие сведения о безопасности компьютерных систем, проведении ее анализа

Тезисы лекции:

- Понятие многоуровневой защиты.
- Основные механизмы обеспечения сетевой безопасности. Модель многоуровневой защищенной корпоративной сети. Защита от атак в ЛВС.
- Основные элементы архитектуры межсетевых экранов. Технология фильтрации пакетов межсетевых экранов. Технология контроля состояний межсетевых экранов. Технология унифицированного межсетевого экранирования. Основные схемы подключения межсетевых экранов. Технология PVLAN.
- Сущность аудита информационной безопасности. Внешний и внутренний аудит. Необходимость и актуальность аудита безопасности. Постановка проблемы аудита безопасности.
- Общая характеристика критериев аудита информационной безопасности.
- Основные нормативные документы, используемые при организации аудита. Национальные и отраслевые стандарты безопасности компьютерных систем.
- Особенности автоматизированных информационных систем как объектов аудита ИБ.
- Основные характеристики информационного и организационно-методического обеспечения безопасности функционирования организаций.

Слайды презентации к лекции:

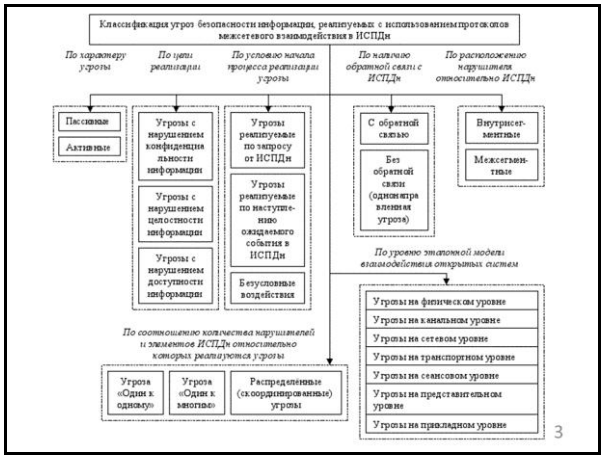
Общие сведения о безопасности компьютерных систем, проведении ее анализа

Дисциплина: Анализ безопасности компьютерных систем

Основные понятия

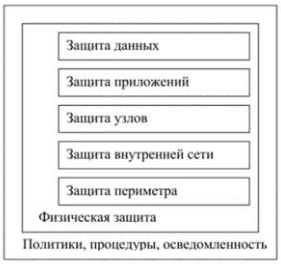
Под безопасностью информации понимается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.
Ущерб безопасности подразумевает нарушение состояния защищенности содержащейся в вычислительной системе информации путем осуществления несанкционированного доступа к объектам вычислительной системы.
Несанкционированный доступ определяется как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых вычислительными системами. Можно ввести более простое определение несанкционированному доступу: несанкционированный доступ заключается в получении пользователем или программой доступа к объекту, разрешение на который в соответствии с принятой в системе политикой безопасности отсутствует.
Реализация угрозы называется атакой. Человек, стремящийся реализовать угрозу, называется нарушителем, или злоумышленником.

2



3

Модель многоуровневой защиты



4

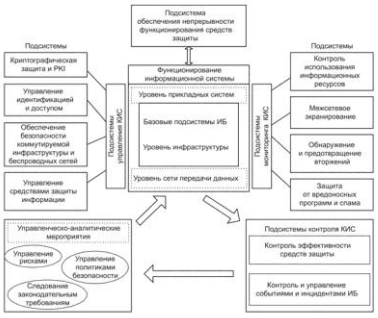
Механизмы обеспечения сетевой безопасности

В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

5

Многоуровневый подход к обеспечению безопасности КИС



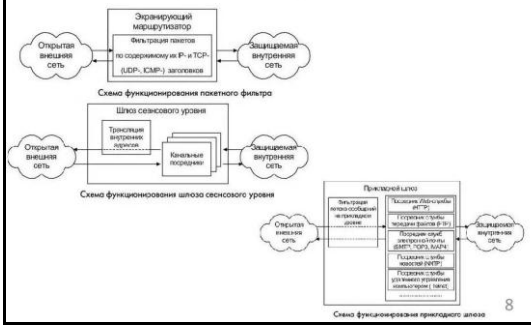
6

Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI



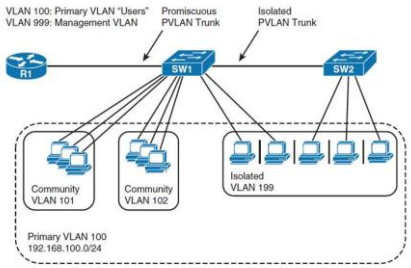
7

Особенности функционирования межсетевых экранов на различных уровнях модели OSI



8

Технология PVLAN



9

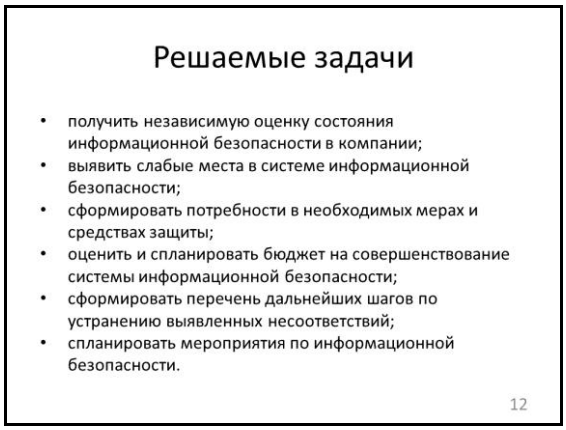
Аудит информационной безопасности

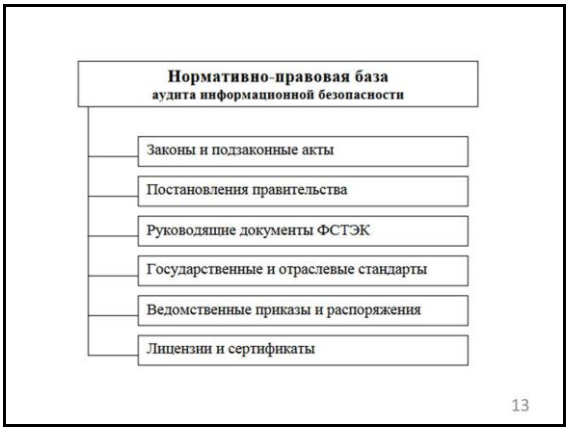
Системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности.

10



11







Литература: Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 100 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1277-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

Лекция 2. Содержание работ при аудите безопасности информационных систем

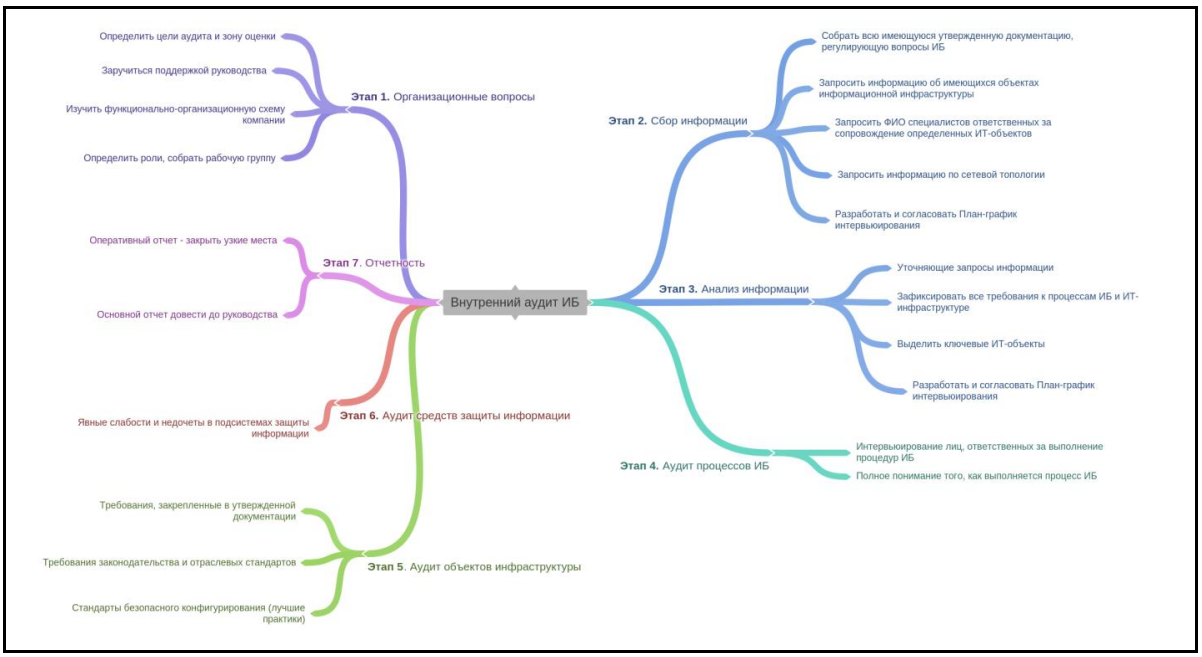
Тезисы лекции:

- Цели и виды аудита информационной безопасности. Основные этапы работ по проведению аудита безопасности. Этапы проведения аудита. Стадии аудита: планирование; моделирование; тестирование; анализ; разработка предложений; документирование.

- Принципы и формы аудита ИБ. Формы обследования (аудита): первоначальное обследование (первичный аудит); предпроектное обследование (технический аудит); аттестация объекта; сюрвей; плановое обследование (контрольный аудит). Техника аудита. Ведение записей. Основные и дополнительные задачи внутреннего аудита безопасности информационных систем.
- Этапы и содержание работ по проведению аудита ИБ. Инициирование процедуры аудита. Подготовка к аудиту и общая схема его проведения. Технология сбора информации аудита. Планирование и осуществление процедуры аудита. Методика подготовки аудитора. Дополнительные задачи, стоящие перед внутренним аудитором. Перечень и состав документов. Сбор свидетельств. Формулирование несоответствий.

Иллюстративный материал к лекции:







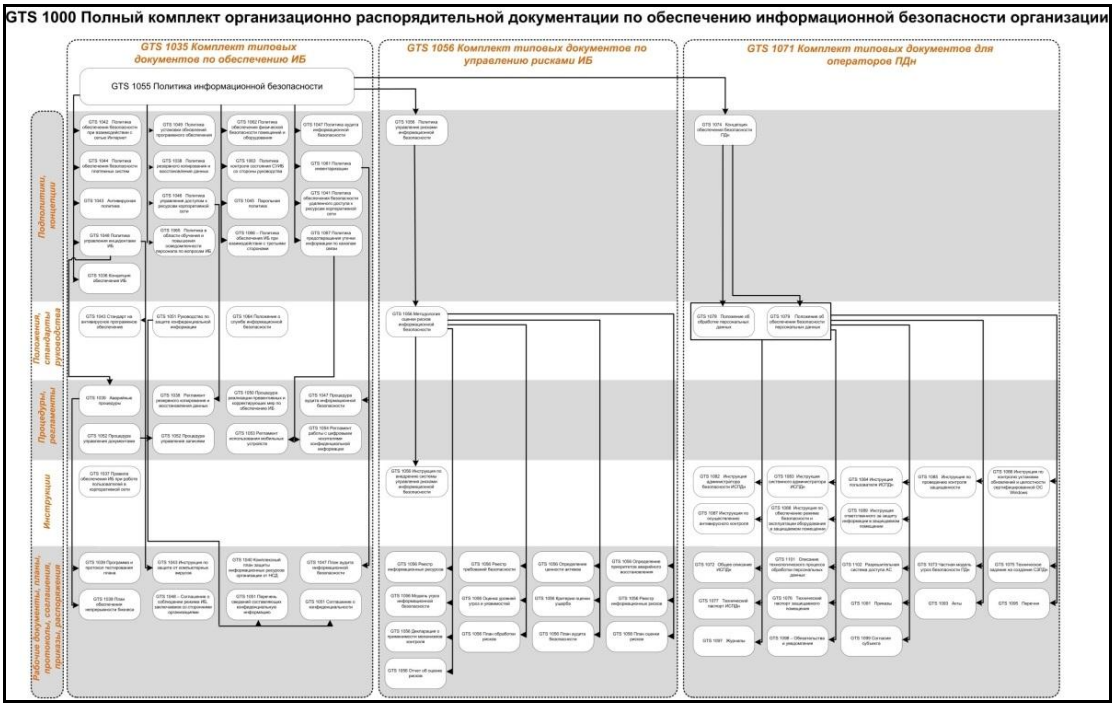
Литература: Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 100 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1277-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

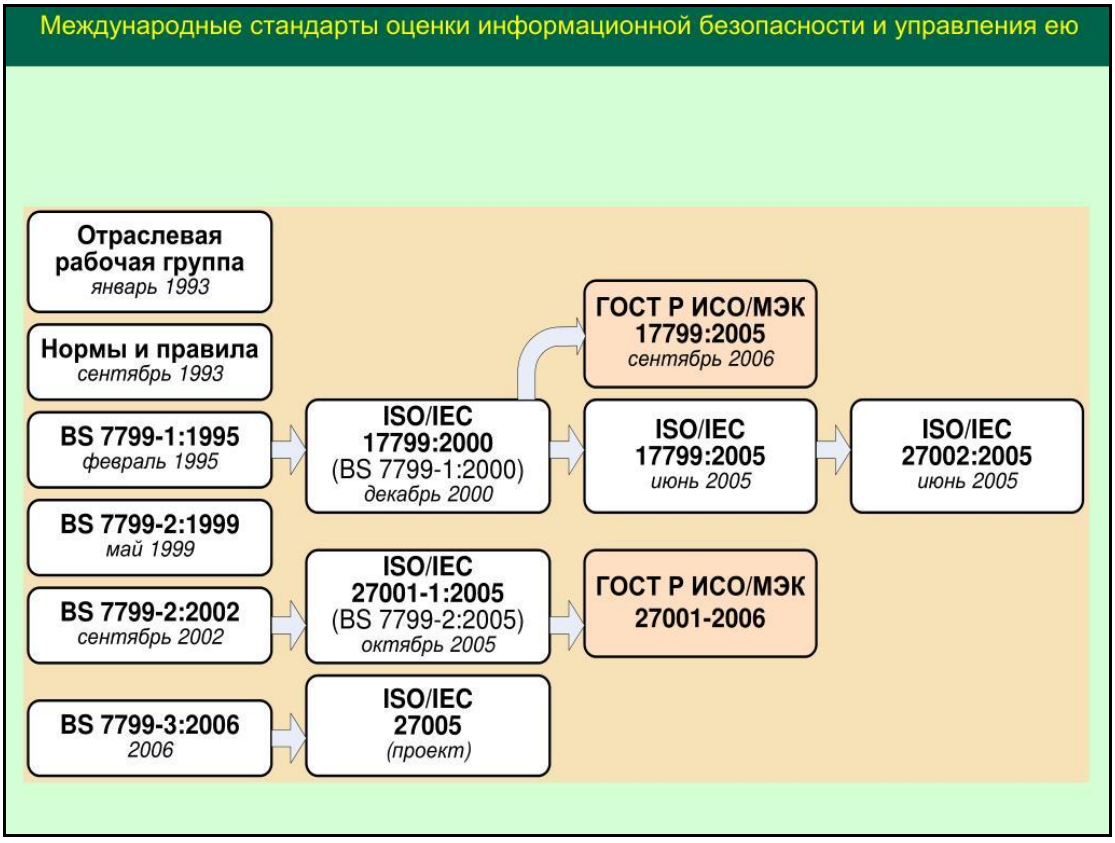
Лекция 3. Методология проведения аудита информационной безопасности

Тезисы лекции:

- Основные подходы к анализу данных. Задачи анализа и управления рисками информационной безопасности. Интервью с сотрудниками организации с использованием заранее подготовленных и стандартизованных опросных листов.
- Оценка состояния информационной безопасности на соответствие стандартам. Обязанности и правила этики аудитора. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы и средства анализа защищенности.
- Документирование системы и анализ рисков с использованием специализированного программного инструментария и шаблонов отчетов.
- Анализ организационно-распорядительной документации по обеспечению режима информационной безопасности.
- Оценка процессов обеспечения информационной безопасности в организации, квалификации сотрудников, знания ими своих должностных обязанностей и степени их осведомленности в вопросах информационной безопасности.
- Оценка достаточности физических механизмов безопасности. Обоснование требований по результатам оценки рисков.

Иллюстративный материал к лекции:





Информационная безопасность в ITIL

Структура ISO 27002 (бывший ISO 17799)

1. **Security Policy** (1) – политика безопасности;
2. **Organizing Information Security** (2) – организация ИБ;
3. **Asset Management** (2) – управление активами;
4. **Human Resources Security** (3) – управление персоналом;
5. **Physical and Environmental Security** (2) – физическая безопасность и безопасность окружения;
6. **Communications and Operations Management** (10) – управление коммуникациями и операциями;
7. **Access Control** (7) – управление доступом;
8. **Information Systems Acquisition, Development and Maintenance** (6) – приобретение, разработка и поддержка информационных систем;
9. **Information Security Incident Management** (2) – управление инцидентами ИБ;
10. **Business Continuity Management** (1) – управление непрерывностью бизнеса;
11. **Compliance** (3) – соответствие законодательству.

Альтернативный перевод ISO 27002 – http://bezpeka.ladimir.kiev.ua – Методология.

Информационная безопасность в ITIL

Управление рисками – дальнейшее развитие ИБ.

Отчет по анализу рисков – основной документ при управлении рисками.



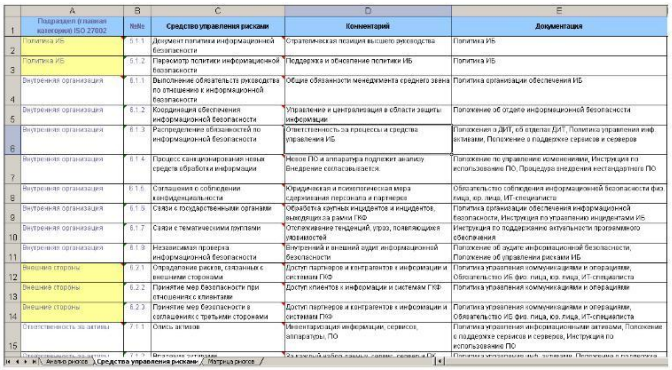
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Код риска	Группа активов	Угроза	целостность	доступность	конфиденц.	ВСЕМЕСТО	Уязвимости	Ценность группы активов	Дата оценки в группе	Кол-во требований ИБ	Ценность актива	Степень ущерб. простоя в осущ. угрозы	Вероятность (статист. + мировой опыт)	Риск-фактор
2	3	Документы / Информация	Сбой резервирования. Авария в системе резервного копирования, повреждение лент	+	+		+	Чувствительность носителей данных к повреждениям, конс / дефекты оборудования	4	2	2	9	4	4	144
3	10	Документы / Информация	Повреждение жестких дисков	+	+			Чувствительность носителей данных к повреждениям	4	3	2	9	4	4	144
4	82	Сервисы	Неуправляемые конфигурации. Снижение эффективности управления ИТ-процессами из-за отсутствия сведений о конфигурации		-			Неадекватное управление конфигурацией	4	4	1	9	4	4	144
5	28	Оборудование	Отказ ядра сети. Выход из строя или снижение производительности центрального коммутатора. Зависание коммутационной фабрики.		+		+	Устаревшее / изношенное, некачественное / дефектное оборудование	3	3	1	9	4	3	98
6	29	Оборудование	Аварии электроснабжения. Долговременное отсутствие электропитания в сети		+		+	Нестабильное электропитание, неполадки и неадекватное управление дизель-генераторами аварийных состояния, топливо)	3	4	1	9	3	3	81
7	86	Сервисы	Отказ 1С		+		+	Неадекватное управление ошибки, недостатки оборудованием, ОС, СУБД, устаревшее / дефектное оборудование	4	3	1	9	3	3	81
8	88	Сервисы	Отказ ERP		+		+	Неадекватное управление ошибки, недостатки оборудованием, ОС, кластером, СУБД, устаревшее / дефектное оборудование	4	3	1	9	3	3	81
9	36	Оборудование	Неавторизованное оборудование. Снижение безопасности сети вследствие подключения неавторизованного / небезопасного оборудования			-		Отсутствие аутентификации оборудования, отсутствие карантина для небезопасного оборудования, наличие пользовательских, внешних точек доступа	3	1	1	5	4	4	80

Анализ рисков / Средства управления рисками / Матрица рисков /

Информационная безопасность в ITIL

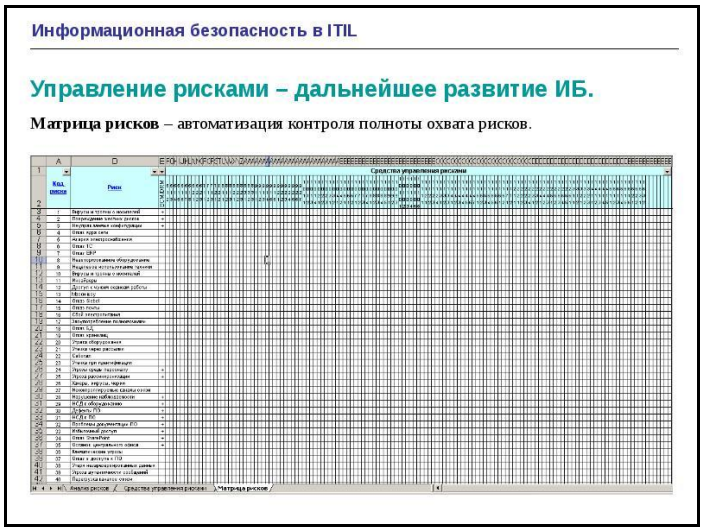
Управление рисками – дальнейшее развитие ИБ.

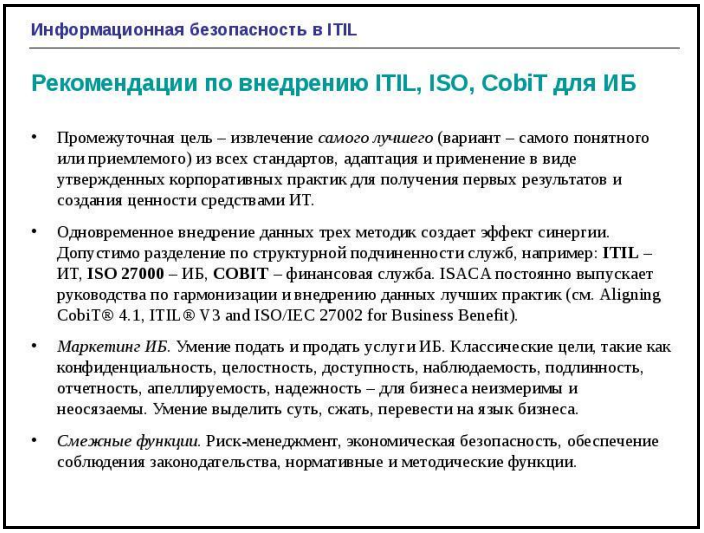
Средства управления (controls) = Положение о применимости согласно ISO 27001.



	A	B	C	D	E
1	Подраздел (глава) категории ISO 27002	Note	Средство управления рисками	Комментарий	Документация
2	Политика ИБ	5.1.1	Документ политики информационной безопасности	Стратегическая позиция высшего руководства	Политика ИБ
3	Политика ИБ	5.1.2	Пересмотр политики информационной безопасности	Поддержка и обеспечение политики ИБ	Политика ИБ
4	Внутренняя организация	6.1.3	Выполнение обязательств руководства по отношению к информационной безопасности	Общие обязанности менеджмента среднего звена	Политика организации обеспечения ИБ
5	Внутренняя организация	6.1.2	Координация обеспечения информационной безопасности	Управление и централизация в области защиты информации	Положение об отделе информационной безопасности
6	Внутренняя организация	6.1.3	Распределение обязанностей по информационной безопасности	Ответственность за процессы и средства управления ИБ	Положения о ДИТ, об отделе ДИТ, Политика управления инф. активами, Положение о поддержке сервисов и серверов
7	Внутренняя организация	6.1.4	Процесс санкционирования новых средств обработки информации	Новое ПО и аппаратура подлежит анализу. Внедрение согласовывается	Положение по управлению изменениями, Инструкция по использованию ПО, Процедура внедрения нестандартного ПО
8	Внутренняя организация	6.1.5	Соглашения о соблюдении конфиденциальности	Юридическая и психологическая мера сдерживания персонала и партнеров	Обязательство соблюдения информационной безопасности физ. лица, юр. лица, ИТ-специалисты
9	Внутренняя организация	6.1.6	Связи с государственными органами	Обработка крупных инцидентов и инцидентов, выходящих за рамки ГКФ	Политика организации обеспечения информационной безопасности, Инструкция по управлению инцидентами ИБ
10	Внутренняя организация	6.1.7	Связи с тематическими группами	Отслеживание тенденций, угроз, появляющихся уязвимостей	Инструкция по поддержанию актуальности программного обеспечения
11	Внутренняя организация	6.1.9	Независимая проверка информационной безопасности	Внутренний и внешний аудит информационной безопасности	Положение об аудите информационной безопасности, Положение об управлении рисками ИБ
12	Внешние стороны	6.2.1	Определение рисков, связанных с внешними сторонами	Доступ партнеров и контрагентов к информации и системам ГКФ	Политика управления коммуникациями и операциями, Обязательство ИБ физ. лица, юр. лица, ИТ-специалисты
13	Внешние стороны	6.2.2	Понятие мер безопасности при отношениях с клиентами	Доступ клиентов к информации и системам ГКФ	Политика управления коммуникациями и операциями
14	Внешние стороны	6.2.3	Понятие мер безопасности в соглашениях с третьими сторонами	Доступ партнеров и контрагентов к инфомации и системам ГКФ	Политика управления коммуникациями и операциями, Обязательство ИБ физ. лица, юр. лица, ИТ-специалисты
15	Ответственность за активы	7.1.1	Опись активов	Инвентаризация информации, сервисов, аппаратуры, ПО	Политика управления информационными активами, Положение о поддержке сервисов и серверов, Инструкция по использованию ПО

Анализ рисков / Средства управления рисками / Матрица рисков /





Литература: Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 100 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1277-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

Лекция 4. Отчёт об аудите безопасности АИС

Тезисы лекции:

- Методика подготовки отчётных документов после проведенного аудита, структура и содержание отчёта.
- Рекомендации организации, предприятию по результатам аудита.
- Оформление общего отчета.
- Представление о степени профессиональной квалификации аудитора.
- Законодательная и нормативная база аудита ИБ.
- Классификация уязвимостей АИС.

Слайды презентации к лекции:



1. Физический контроль доступа в помещения, наблюдение за помещениями

Анализ сферы физического доступа, наблюдения и контроля помещений на объекте Заказчика

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Контроль физического доступа в помещения в рабочее и нерабочее время	**Центральный офис** Два простых аппаратных контроллера электронных ключей, запрограммированы на открытие электронного входного замка каждой двери по карточке доступа, без логической составляющей, в любое время суток **Склад** Закрывается на ключ	СКУД – отдельная интеллектуальная система управления доступом, базированная на собственном сервере, к которой по сети IP подключены контроллеры доступа каждого отдельного помещения: • Серверная • Кабинеты руководителей • Кабинеты изолированных отделов	• Нет системы гибкого управления физическим доступом • Все внутренние отдельные помещения физически защищены обыкновенными замками, некоторые ключи находятся в свободном доступе	• Закупить отдельный сервер • Закупить ПО СКУД • Закупить и установить контроллеры и электронные замки для каждого отдельного помещения • Подключить контроллеры дверей к центральной системе СКУД • Настроить систему СКУД согласно техническому заданию, с учетом разрешенных уровней доступа групп сотрудников и времени суток

2

2. Аппаратное обеспечение информационной системы

Анализ серверной и центральной коммутационной структуры, физической доступности рабочих станций и периферийного оборудования

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Защищенность помещения и наличие специальных защитных монтажных изделий, в которых физически расположена серверная и коммутационная структура	**Центральный офис** • На объекте есть выделенное помещение для работы серверной и центральной коммутационной структуры. • Помещение защищено замком. • Серверная стойка открытая. • Помимо серверного оборудования, помещение служит хранилищем пустой тары от офисной электронной техники **Склад** • На объекте нет никаких защитных помещений либо шкафов, все оборудование размещено в мебельной тумбе • Тумба открывается без ключей	• На объекте должно быть выделенное помещение с четко ограниченным доступом сотрудникам согласно регламента безопасности Или • На объекте должен быть защищенный серверный шкаф, ключи должны находиться у ответственного лица • Должны быть запрещены прямые консольные выводы (типа розеток питания, мониторов, клавиатур, KVM и т.д.) за пределы защищенного серверного шкафа либо полки • Серверная комната не должна использоваться в качестве склада и других	Ключи от серверной комнаты лежат у ИТ-инженера в ящике стола. В принципе есть возможность попасть в серверную любому сотруднику либо гостю Серверная стойка открытая, комната совмещена со складом тары. Есть риск повреждения центральных коммуникаций либо серверного оборудования при проведении хоз. работ	• Внедрить систему СКУД с четким разграничением доступа к серверной комнате (см. пункт 1) • Как бюджетный вариант - организация полностью закрытого монтажного изделия, содержащего серверную и коммуникационную структуры, без возможности намеренного или ненамеренного влияния посторонних лиц

3

3. Сетевое обеспечение информационной системы

Анализ кабельной структуры Организации, доступности и защищенности сетевых розеток и беспроводных соединений

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Наличие общедоступных участков кабельной системы с возможностью неконтролируемого подключения спец устройств	**Центральный офис** • Сеть сделана по проекту специализированной компании • Проектная документация присутствует • Структурированная документация и схема сети • В сети присутствует защита методом назначения сервером DHCP разных данных в зависимости от подключения к той или иной сетевой розетке. Однако данная схема не контролирует адреса, проставленные злоумышленником вручную. **Склад** • Проектировки сетевой структуры нет • Информационная и электрическая	• Структура должна соответствовать стандартам построения кабельных сетей • Структура должна иметь разделенную физически пользовательскую область и демилитаризированные зоны с контролем обмена траффиком между ними	• Нет фильтрации сетевых портов по MAC-адресам устройств • Есть общественные сетевые розетки • Нет разделения сети на Vlan и демилитаризованные зоны. Злоумышленник, подключившись со статическим адресом к общедоступной сетевой розетке может получить доступ к локальной сети **Склад** Структура полностью не соответствует требованиям безопасности	• Необходимо внедрить привязку сетевых портов к разрешенным MAC-адресам. Оставить только контролируемые порты, например в конференц-зале. • Все неиспользуемые сетевые разъемы должны быть физически отключены, заглушены либо деактивированы на патч-панелях в серверном шкафу • Данные сетевые порты вывести в отдельный Vlan в демилитаризованной гостевой зоне с разграничением доступа через Firewall согласно ТЗ **Склад** • Необходимо рассчитать проект и привести кабельную

4

4. Системное программное обеспечение

Результаты аудита операционных систем серверов, защиты рабочих станций, коммутационного оборудования, маршрутизаторов, степени защиты паролей и резервных копий

Проведение практических тестов:

- Сканирование локальной сети на открытые ресурсы, поиск общедоступных ресурсов
- Подключение к серверным и периферийным устройствам по сети, возможность вывода их из строя
- Проведение сканирования внешних портов, фиксирование точек успешных атак через найденные уязвимости
- Проверка файлов резервных копий, попытка найти, увидеть, открыть, скачать, удалить их под правами пользователя
- Подключиться к сети, вычислить серверные ресурсы, попробовать выложить документы на внешний ресурс

Объект изучения	Нарушения, замечания и угрозы	Меры по исправлению ситуации
000.000.000.000 - точка доступа DIR-615	Можно зайти под пользователем User и пустым паролем, просмотреть всю информацию о пробросах, MAC, пользователях, устройствах в сети и т.д.	Необходимо усилить защиту паролем: • Пароль не должен быть слишком коротким, минимум 7 символов • Пароль должен содержать сочетание нескольких цифирных, буквенных символов и одного спец-символа • Пароль не должен быть словарным словом или простым их сочетанием • Пароль не должен состоять только из общедоступной информации
000.000.000.000 - HP LaserJet P1505n	Можно зайти на веб-интерфейс с пустым	Необходимо усилить защиту паролем:

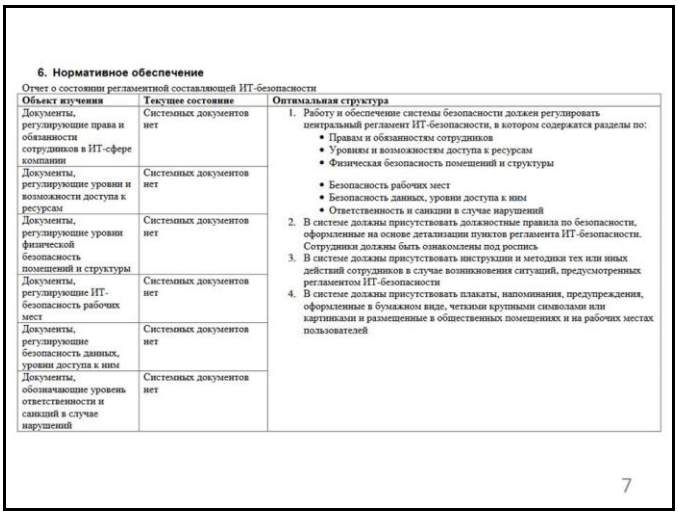
5

5. Организационное обеспечение

Анализ состояния субъектов системы - пользователей, их прав доступа, времени работы в ИТ-системе, мониторинга и отчетности об их действиях

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Возможность доступа к включенной рабочей станции, периферийному оборудованию посторонним лицом либо другим пользователем при отсутствии сотрудника на рабочем месте (вышел по необходимости, на обед, на перекур и т.д.)	• Рабочие станции выключаются по питанию при долгосрочном отсутствии сотрудника • При краткосрочном отсутствии сотрудника рабочие станции, рабочие столы и открытые документы остаются доступными • Экраны не блокируются (за исключением некоторых лиц)	Доступ к операционной среде должен блокироваться вручную при уходе сотрудника с рабочего места либо автоматически по истечению 5 минут простоя операционной среды	Злоумышленник свободно может получить доступ к незащищенному рабочему месту, оставленному без присмотра	Внедрение политики безопасности рабочих мест при отсутствии сотрудника
Пользовательская операционная система и интерфейс пользователя	• Рабочие станции пользователей представляют собой автономные ПК без контроля со стороны доменных структур • Политики ограничения пользовательских прав и ресурсов рабочих мест нет • Ограничений рабочих	• ОС пользователей должна быть ограничена только нужным функционалом,. Уровень ограничения операционной среды (например, интерфейса Microsoft Windows) должен соответствовать группам доступа пользователей и быть	Свободный круг возможностей, особенно с правами администратора, в операционной среде пользователя дает широкую возможность действия вирусов, троян-инъекций, хакеров, неосторожных действий пользователей в операционной системе и	• Создание и внедрение регламента безопасности с четкими политиками ограничения рабочих мест пользователей, регулированием работы по времени суток с помощью функционала домена

6

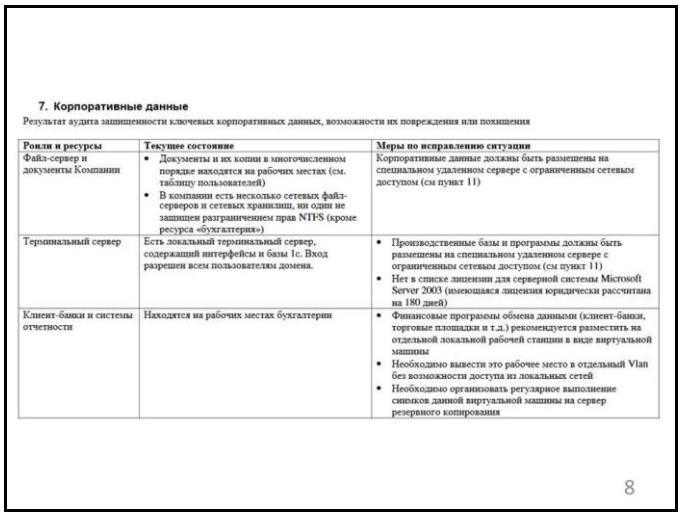


6. Нормативное обеспечение

Отчет о состоянии регламентной составляющей ИТ-безопасности

Объект изучения	Текущее состояние	Оптимальная структура
Документы, регулирующие права и обязанности сотрудников в ИТ-сфере компании	Системных документов нет	1. Работу и обеспечение системы безопасности должен регулировать центральный регламент ИТ-безопасности, в котором содержатся разделы по: • Правам и обязанностям сотрудников • Уровням и возможностям доступа к ресурсам • Физическая безопасность помещений и структуры • Безопасность рабочих мест • Безопасность данных, уровни доступа к ним • Ответственность и санкции в случае нарушений 2. В системе должны присутствовать должностные правила по безопасности, оформленные на основе детализации пунктов регламента ИТ-безопасности. Сотрудники должны быть ознакомлены под роспись 3. В системе должны присутствовать инструкции и методики тех или иных действий сотрудников в случае возникновения ситуаций, предусмотренных регламентом ИТ-безопасности 4. В системе должны присутствовать плакаты, напоминания, предупреждения, оформленные в бумажном виде, четкими крупными символами или картинками и размещенные в общественных помещениях и на рабочих местах пользователей
Документы, регулирующие уровни и возможности доступа к ресурсам	Системных документов нет	
Документы, регулирующие уровни физической безопасность помещений и структуры	Системных документов нет	
Документы, регулирующие ИТ-безопасность рабочих мест	Системных документов нет	
Документы, регулирующие безопасность данных, уровни доступа к ним	Системных документов нет	
Документы, обозначающие уровень ответственности и санкций в случае нарушений	Системных документов нет	

7



7. Корпоративные данные

Результат аудита защищенности ключевых корпоративных данных, возможности их повреждения или похищения

Роли и ресурсы	Текущее состояние	Меры по исправлению ситуации
Файл-сервер и документы Компании	• Документы и их копии в многочисленном порядке находятся на рабочих местах (см. таблицу пользователей) • В компании есть несколько сетевых файл-серверов и сетевых хранилищ, ни один не защищен разграничением прав NTFS (кроме ресурса «бухгалтерия»)	Корпоративные данные должны быть размещены на специальном удаленном сервере с ограниченным сетевым доступом (см пункт 11)
Терминальный сервер	Есть локальный терминальный сервер, содержащий интерфейсы и базы 1с. Вход разрешен всем пользователям домена.	• Производственные базы и программы должны быть размещены на специальном удаленном сервере с ограниченным сетевым доступом (см пункт 11) • Нет в списке лицензии для серверной системы Microsoft Server 2003 (имеющаяся лицензия юридически рассчитана на 180 дней)
Клиент-банки и системы отчетности	Находятся на рабочих местах бухгалтерии	• Финансовые программы обмена данными (клиент-банки, торговые площадки и т.д.) рекомендуется разместить на отдельной локальной рабочей станции в виде виртуальной машины • Необходимо вывести это рабочее место в отдельный Vlan без возможности доступа из локальных сетей • Необходимо организовать регулярное выполнение снимков данной виртуальной машины на сервер резервного копирования

8



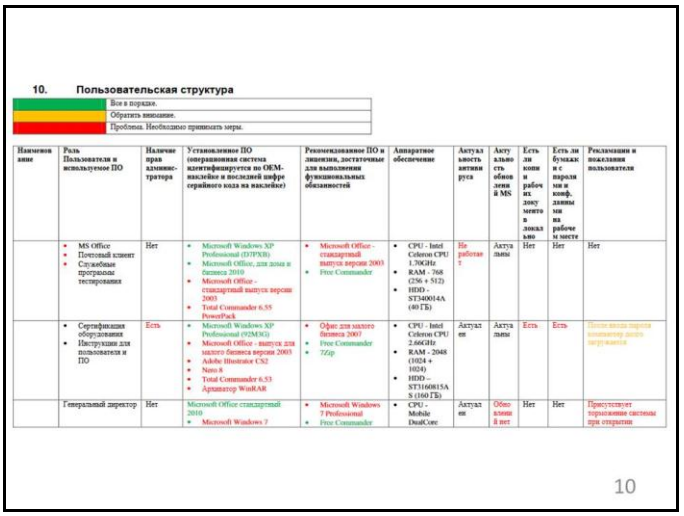
8. Внутренняя IT-структура – СКС, интрасетевые устройства, коммутационные устройства

№	IP адрес	Название устройства	Описание
1			Телевизор Samsung 55 inch conference room
2			Телевизор Samsung 32 inch doccenter
3			Телевизор Samsung 55 inch showroom
4			Медиацентр Iconbit
5			Принтер HPM2037
6			Принтер Kyocera
7			Принтер HP_color
8			Принтер Panasonic
9			Точка доступа WIFI №1
10			Точка доступа WIFI №2
11			Точка доступа WiFi Dlink

9. Серверная IT-структура — сервера и их роли в системе компании

№	IP адрес	Название устройства	Роли	Ресурсы
1			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5405 6 Gb Raid5 500 GB
3			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5405 6 Gb RAID5 1.8 Tb
4			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5335 4 Gb Raid5 500 GB

9

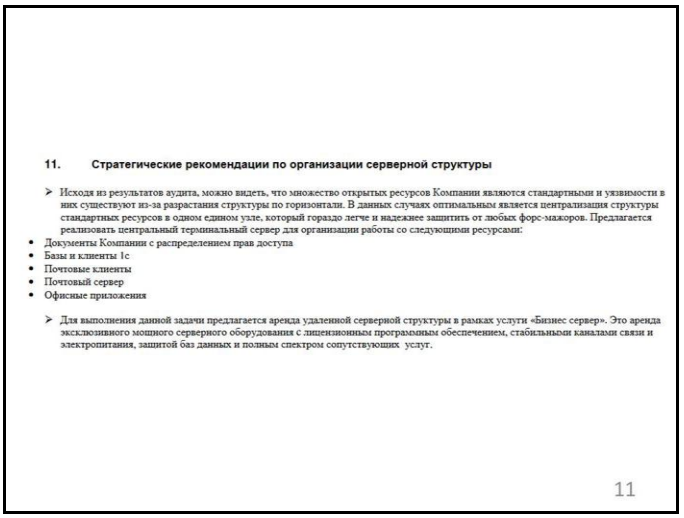


10. Пользовательская структура

	Все в порядке.
	Обратить внимание.
	Проблема. Необходимо принимать меры.

Наименование	Роль Пользователи и используемое ПО	Наличие прав администратора	Установленное ПО (операционная система идентифицируется по OEM-наклейке и последней цифре серийного кода на наклейке)	Рекомендованное ПО и лицензии, достаточные для выполнения функциональных обязанностей	Аппаратное обеспечение	Актуальность антивируса	Актуальность обновлений MS	Есть ли копии рабочих документов локально	Есть ли бумажные с паролями и конф. данными на рабочем месте	Рекламации и пожелания пользователя
	• MS Office • Почтовый клиент • Служебные программы тестирования	Нет	• Microsoft Windows XP Professional (DTPKB) • Microsoft Office, для дома и бизнеса 2010 • Microsoft Office - стандартный выпуск версии 2003 • Total Commander 6.55 PowerPack	• Microsoft Office - стандартный выпуск версии 2003 • Free Commander	• CPU - Intel Celeron CPU 1.70GHz • RAM - 768 (256 + 512) • HDD - ST340014A (40 ГБ)	Не работает	Актуальны	Нет	Нет	Нет
	• Сертификация оборудования • Инструкции для пользователя и ПО	Есть	• Microsoft Windows XP Professional (92M3G) • Microsoft Office - выпуск для малого бизнеса версии 2003 • Adobe Illustrator CS2 • Nero 8 • Total Commander 6.53 • Архиватор WinRAR	• Офис для малого бизнеса 2007 • Free Commander • 7Zip	• CPU - Intel Celeron CPU 2.66GHz • RAM - 2048 (1024 + 1024) • HDD - ST3160815AS (160 ГБ)	Актуален	Актуальны	Есть	Есть	После ввода пароля компьютер долго загружается
	Генеральный директор	Нет	Microsoft Office стандартный 2010 • Microsoft Windows 7	• Microsoft Windows 7 Professional • Free Commander	• CPU - Mobile DualCore	Актуален	Обновлений нет	Нет	Нет	Присутствует торможение системы при открытии

10



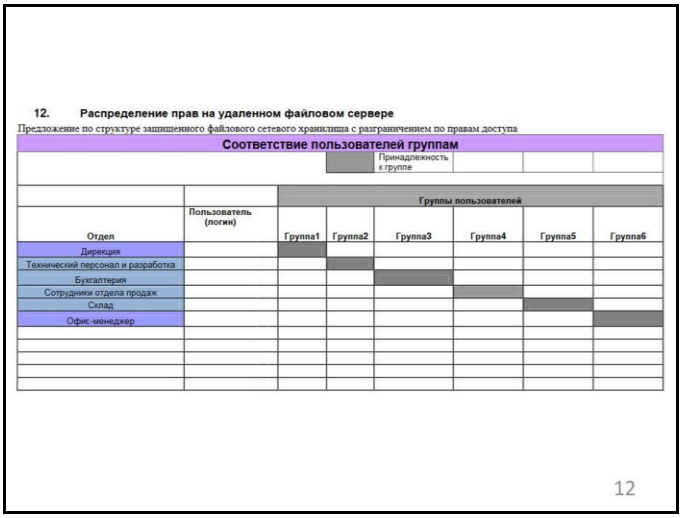
11. Стратегические рекомендации по организации серверной структуры

➢ Исходя из результатов аудита, можно видеть, что множество открытых ресурсов Компании являются стандартными и уязвимости в них существуют из-за разрастания структуры по горизонтали. В данных случаях оптимальным является централизация структуры стандартных ресурсов в одном едином узле, который гораздо легче и надежнее защитить от любых форс-мажоров. Предлагается реализовать центральный терминальный сервер для организации работы со следующими ресурсами:

- Документы Компании с распределением прав доступа
- Базы и клиенты 1с
- Почтовые клиенты
- Почтовый сервер
- Офисные приложения

➢ Для выполнения данной задачи предлагается аренда удаленной серверной структуры в рамках услуги «Бизнес сервер». Это аренда эксклюзивного мощного серверного оборудования с лицензионным программным обеспечением, стабильными каналами связи и электропитания, защитой баз данных и полным спектром сопутствующих услуг.

11



12. Распределение прав на удаленном файловом сервере

Предложение по структуре защищенного файлового сетевого хранилища с разграничением по правам доступа

Соответствие пользователей группам

Принадлежность к группе

Отдел	Пользователь (логин)	Группы пользователей					
		Группа1	Группа2	Группа3	Группа4	Группа5	Группа6
Дирекция							
Технический персонал и разработка							
Бухгалтерия							
Сотрудники отдела продаж							
Склад							
Офис-менеджер							

12

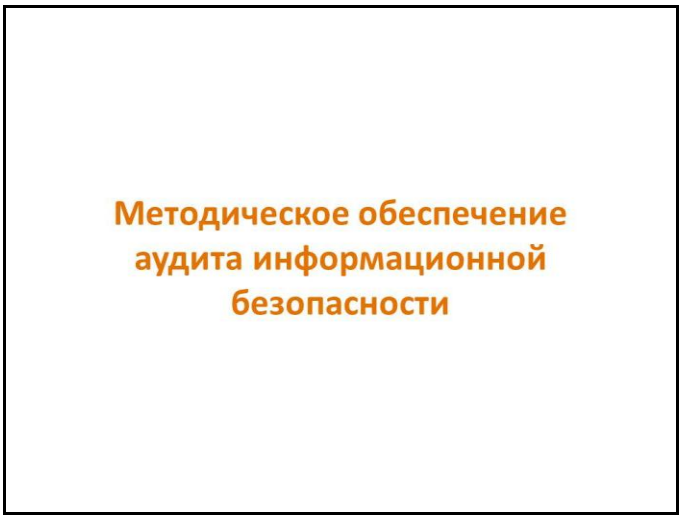
Литература: Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и

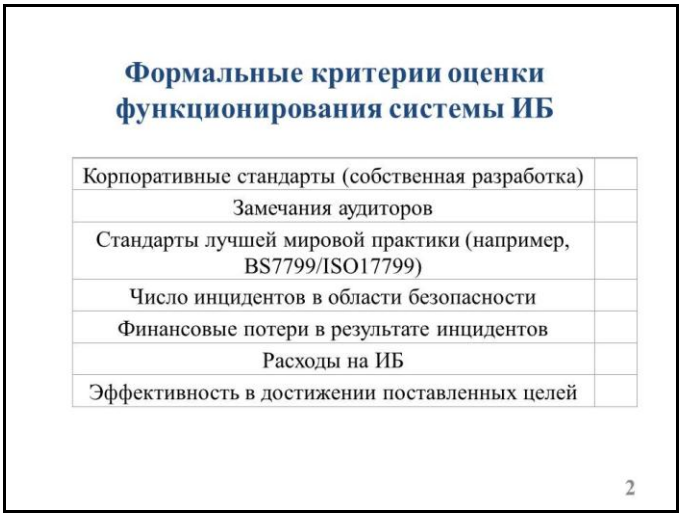
радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637

Лекция 5. Методическое обеспечение аудита информационной безопасности

Тезисы лекции:

- Методы и подходы к управлению рисками информационной безопасности.
- Выявление и оценка угроз, уязвимостей, возможного ущерба. Выбор стратегий управления рисками.
- Обзор современных программных средств анализа и управления рисками информационной безопасности.
- Документация системы управления информационной безопасностью. Выбор стратегии управления рисками ИБ. Обоснование необходимых мер безопасности.





Концепция ISO 17799
(Code of Practice of Information Security Management)

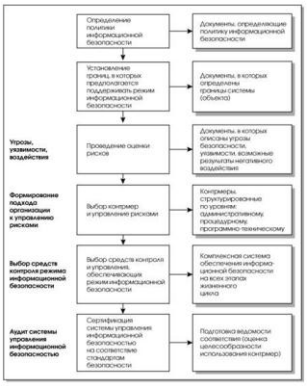


Особенности:
- **Стандарт представляет собой набор качественных рекомендаций**
- **Методики аудита разрабатываются заинтересованными организациями**
- **Рад важных и трудоемких этапов в стандарте не специфицирован (анализ бизнес-процессов, анализ рисков)**

3

Схема аудита в соответствии с BS 7799

Документация должна содержать:
- **политику безопасности;**
- **границы защищаемой системы;**
- **оценки рисков;**
- **управление рисками;**
- **описание инструментария управления ИБ;**
- **ведомость соответствия — документ, в котором оценивается соответствие требованиям стандартов поставленных целей в области ИБ и средств управления ИБ.**



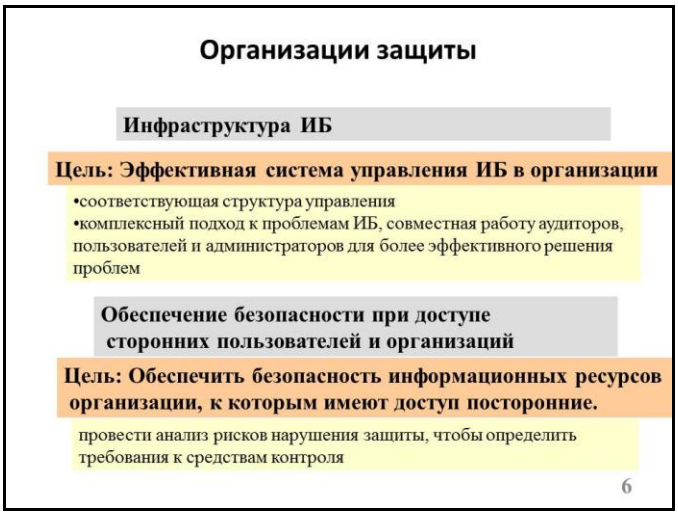
4

Политика информационной безопасности

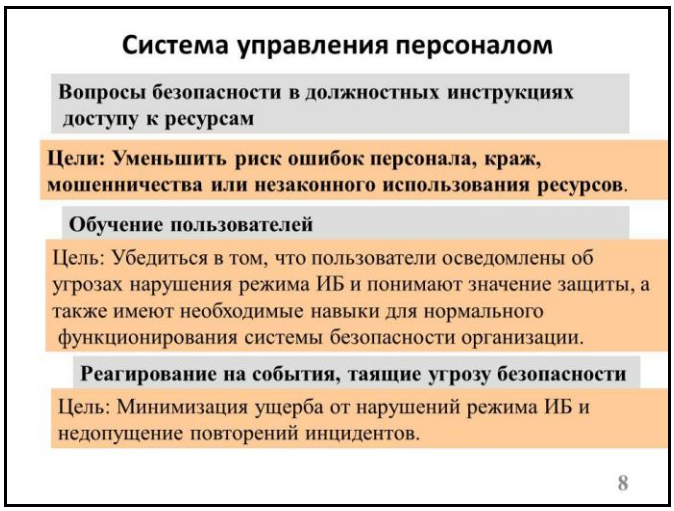
Цель: Сформулировать цель и обеспечить поддержку мер в области информационной безопасности со стороны руководства организации

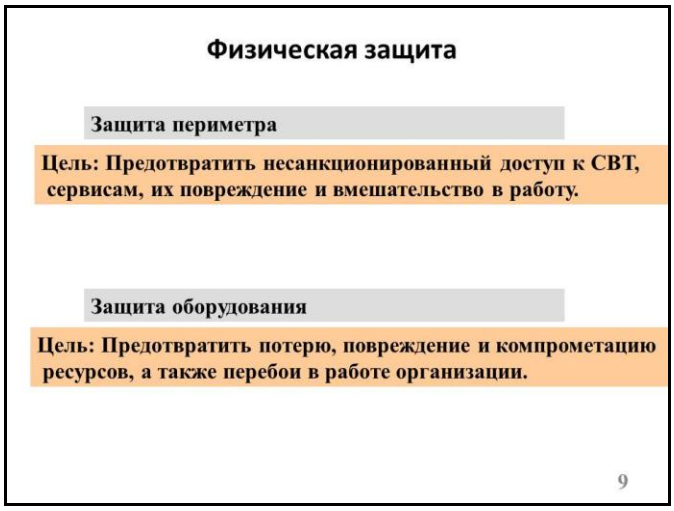
Документ, в котором изложена политика ИБ, должен быть доступен всем сотрудникам, отвечающим за обеспечение режима ИБ. Должны быть рассмотрены следующие вопросы:
- определение ИБ;
- причины, по которым ИБ имеет большое значение для организации;
- цели и показатели ИБ, допускающие возможность измерения.

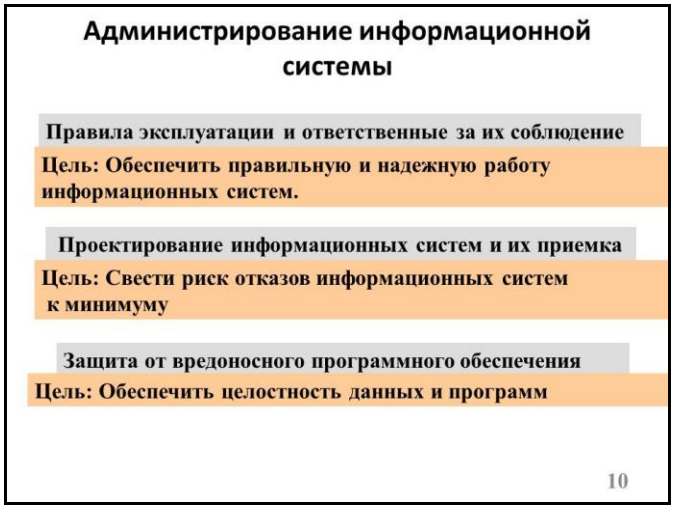
5


Организации защиты
Инфраструктура ИБ
Цель: Эффективная система управления ИБ в организации
•соответствующая структура управления
•комплексный подход к проблемам ИБ, совместная работу аудиторов, пользователей и администраторов для более эффективного решения проблем
Обеспечение безопасности при доступе сторонних пользователей и организаций
Цель: Обеспечить безопасность информационных ресурсов организации, к которым имеют доступ посторонние.
провести анализ рисков нарушения защиты, чтобы определить требования к средствам контроля
6

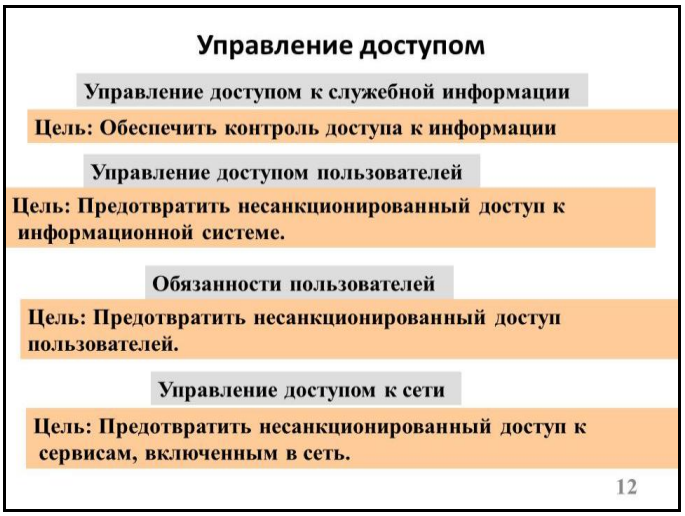

Классификация и управление информационными ресурсами
Ответственность за ресурсы
Цель: Обеспечить надлежащую защиту ресурсов организации. Все основные информационные ресурсы должны быть учтены и иметь ответственных. Кроме того, следует назначить ответственных за реализацию соответствующих защитных мер.
Классификация информации
Цель: Обеспечить надлежащий уровень защиты информационных ресурсов
7

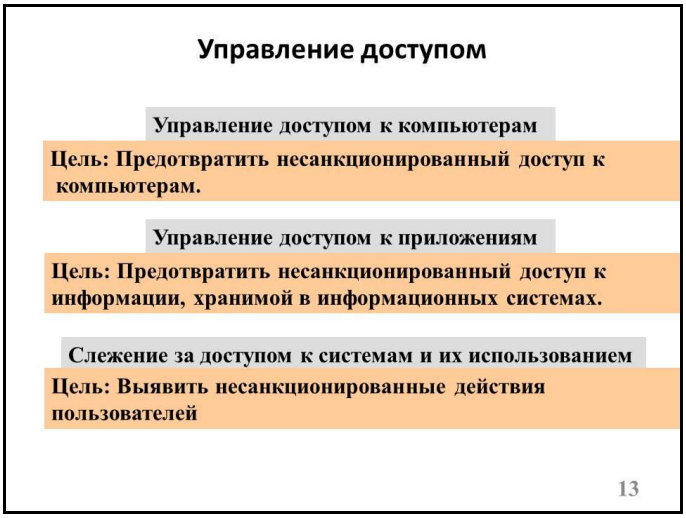

Система управления персоналом
Вопросы безопасности в должностных инструкциях доступу к ресурсам
Цели: Уменьшить риск ошибок персонала, краж, мошенничества или незаконного использования ресурсов.
Обучение пользователей
Цель: Убедиться в том, что пользователи осведомлены об угрозах нарушения режима ИБ и понимают значение защиты, а также имеют необходимые навыки для нормального функционирования системы безопасности организации.
Реагирование на события, таящие угрозу безопасности
Цель: Минимизация ущерба от нарушений режима ИБ и недопущение повторений инцидентов.
8

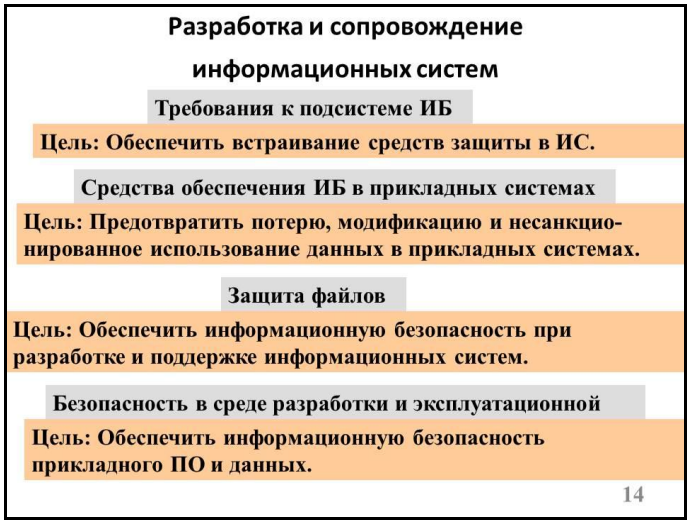

Физическая защита
Защита периметра
Цель: Предотвратить несанкционированный доступ к СВТ, сервисам, их повреждение и вмешательство в работу.
Защита оборудования
Цель: Предотвратить потерю, повреждение и компрометацию ресурсов, а также перебои в работе организации.
9


Администрирование информационной системы
Правила эксплуатации и ответственные за их соблюдение
Цель: Обеспечить правильную и надежную работу информационных систем.
Проектирование информационных систем и их приемка
Цель: Свести риск отказов информационных систем к минимуму
Защита от вредоносного программного обеспечения
Цель: Обеспечить целостность данных и программ
10


Администрирование информационной системы
Обслуживание систем
Цель: Обеспечить целостность и доступность информационных сервисов.
Сетевое администрирование
Цель: Обеспечить защиту информации в сетях
Защита носителей информации
Цель: Предотвратить повреждение информационных ресурсов и перебои в работе организации.
Обмен данными и программным обеспечением
Цель: Предотвратить потери, модификацию и несанкционированное использование данных.
11


Управление доступом
Управление доступом к служебной информации
Цель: Обеспечить контроль доступа к информации
Управление доступом пользователей
Цель: Предотвратить несанкционированный доступ к информационной системе.
Обязанности пользователей
Цель: Предотвратить несанкционированный доступ пользователей.
Управление доступом к сети
Цель: Предотвратить несанкционированный доступ к сервисам, включенным в сеть.
12


Управление доступом
Управление доступом к компьютерам
Цель: Предотвратить несанкционированный доступ к компьютерам.
Управление доступом к приложениям
Цель: Предотвратить несанкционированный доступ к информации, хранимой в информационных системах.
Слежение за доступом к системам и их использованием
Цель: Выявить несанкционированные действия пользователей
13


Разработка и сопровождение информационных систем
Требования к подсистеме ИБ
Цель: Обеспечить встраивание средств защиты в ИС.
Средства обеспечения ИБ в прикладных системах
Цель: Предотвратить потерю, модификацию и несанкционированное использование данных в прикладных системах.
Защита файлов
Цель: Обеспечить информационную безопасность при разработке и поддержке информационных систем.
Безопасность в среде разработки и эксплуатационной
Цель: Обеспечить информационную безопасность прикладного ПО и данных.
14

Планирование бесперебойной работы организации

Вопросы планирования бесперебойной работы организации

Цель: Составить планы предотвращение перебоев в работе организации

15

Проверка на соответствие формальным требованиям

Выполнение требований действующего законодательства

Цель: Избежать нарушений договорных обязательств и требований действующего законодательства при поддержании режима ИБ.

Проверка режима ИБ на соответствие политике безопасности

Цель: Обеспечить соответствие режима ИБ политике и стандартам безопасности организации

Меры безопасности при тестировании

Цель: Минимизировать вмешательство в процесс тестирования и воздействие тестирования на штатную работу.

16

Современные зарубежные технологии аудита ИБ в России

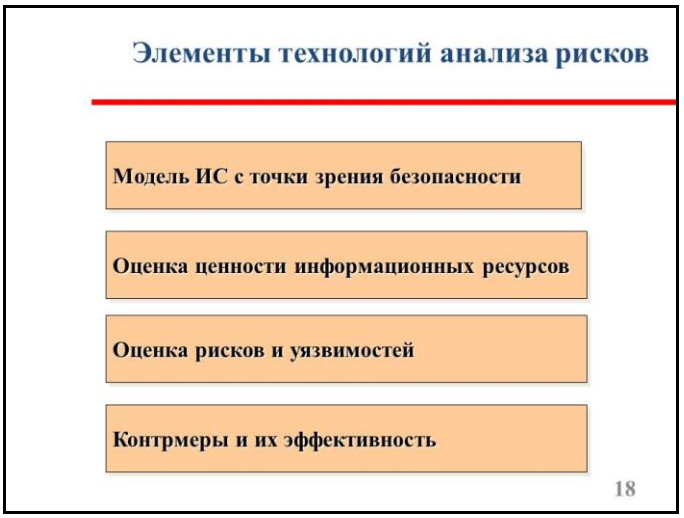
1. **Технологии аудита представляют интерес для реальных собственников информационных ресурсов**

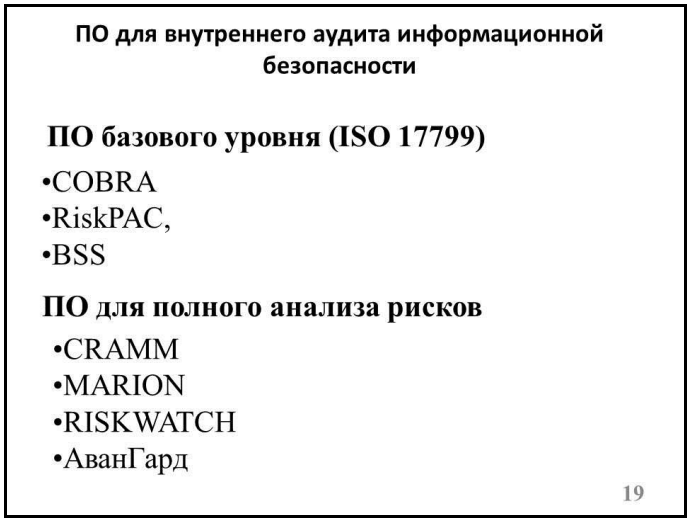
2. **Потенциальные заказчики негативно относятся к привлечению сторонних аудиторов (посторонним не доверяют)**

3. **Наибольший интерес представляют технологии внутреннего аудита, методические материалы, обучение специалистов**

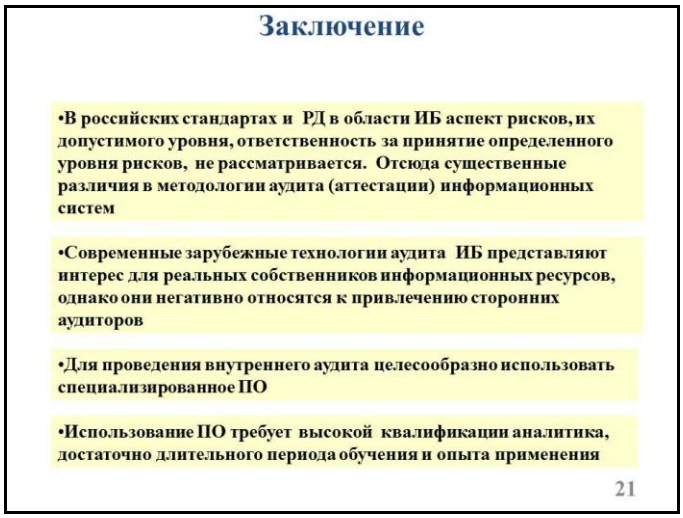
4. **В области методологии наибольший интерес российских специалистов вызывают технологии анализа рисков, позволяющие ответить на следующие вопросы:**
   - **Как составить полный список угроз ИБ и оценить их параметры ?**
   - **Как оценить ценности ресурсов ?**
   - **Как оценнить эффективность контрмер ?**

17


Элементы технологий анализа рисков
Модель ИС с точки зрения безопасности
Оценка ценности информационных ресурсов
Оценка рисков и уязвимостей
Контрмеры и их эффективность
18


ПО для внутреннего аудита информационной безопасности
ПО базового уровня (ISO 17799)
•COBRA
•RiskPAC,
•BSS
ПО для полного анализа рисков
•CRAMM
•MARION
•RISKWATCH
•АванГард
19


Инструментальные средства для анализа рисков
Оценка ценности ресурсов
Выбирается система критериев для оценки ценности ресурсов различных типов с позиции организации
Построение модели с позиции ИБ
Выделяются угрозы и уязвимости, присутствующие в данной ИС
Оценка угроз и уязвимостей
Оценка значений на основе исследования факторов риска с использованием фактографической БД
Измерение рисков
Оценка потенциального вредоносного воздействия на ресурсы: оборудование, данные, ПО
Выбор контрмер
Анализ эффективности возможных вариантов контрмер
Методы: CRAMM, RiskWatch, Авангард
20



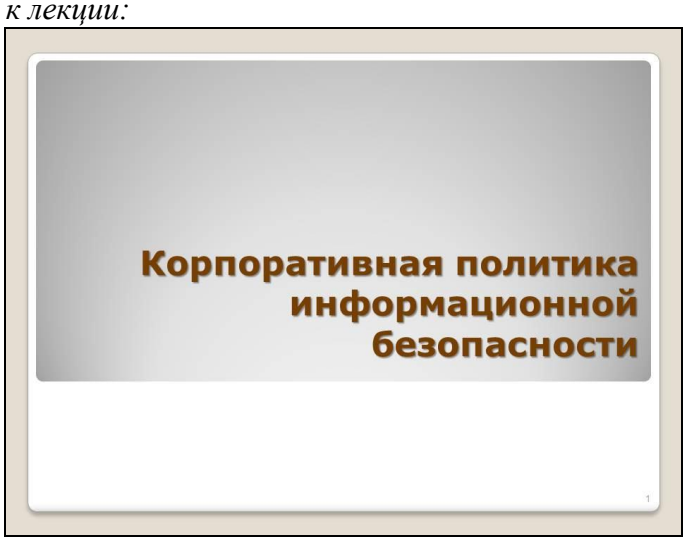
Литература: Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637

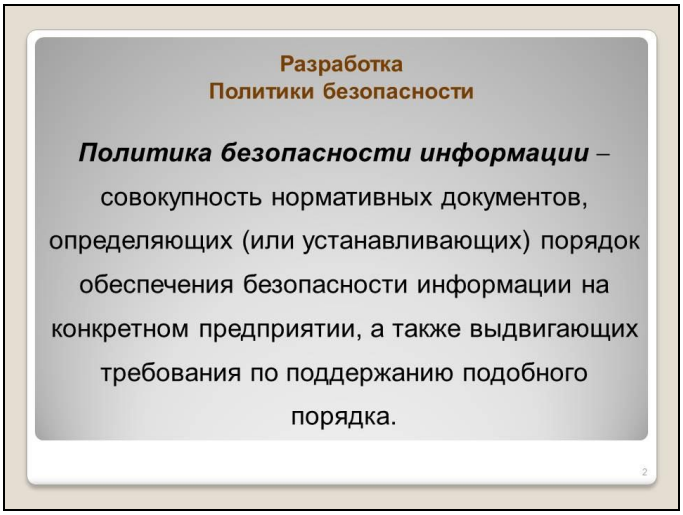
Лекция 6. Корпоративная политика информационной безопасности

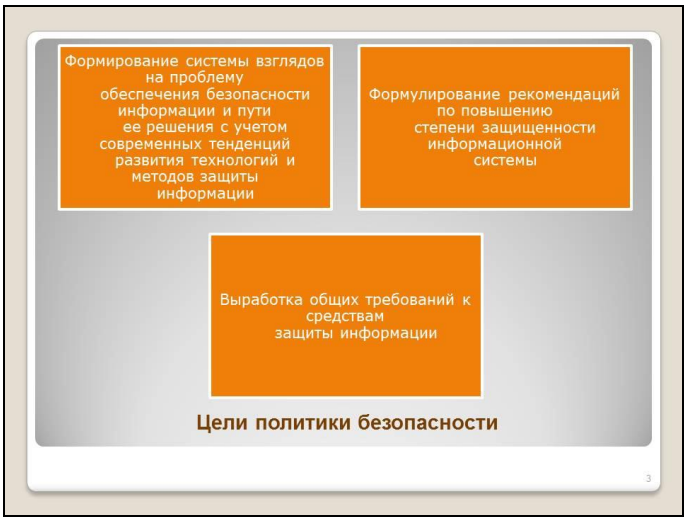
Тезисы лекции:

- Корпоративная политика безопасности; организационно-распорядительные документы организации.
- Формирование политики информационной безопасности организации. Определение требуемого уровня ИБ. Остаточные риски.
- Ядро системы комплексной защиты информации. Ресурсы комплексной системы защиты информации. Интегральные критерии информационной безопасности организации.
- Методы сбора исходных данных. Сбор исходной информации для проведения аудита, такие как: общие исходные данные, исходные данные об обрабатываемой информации, исходные данные о системе обеспечения безопасности информации исходные данные о персонале, сбор дополнительных исходных данных.

Слайды презентации к лекции:



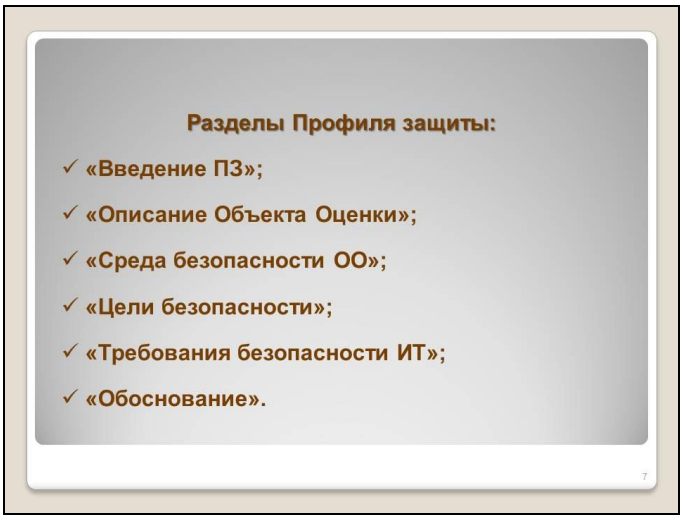




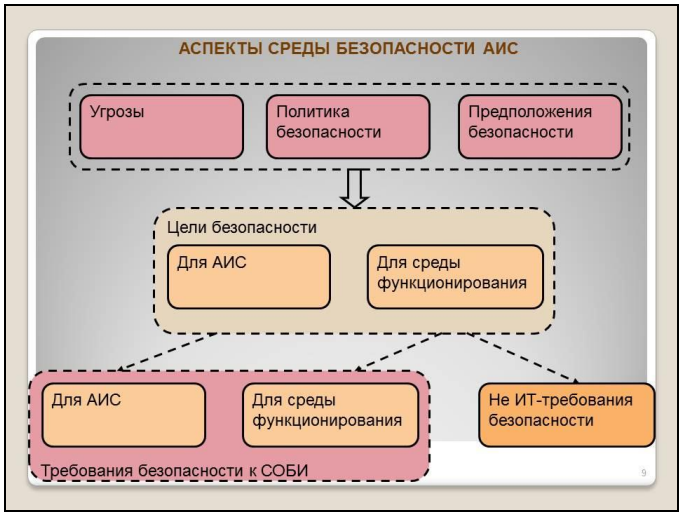

Уровни Политики безопасности информации
Концепция информационной безопасности
Определяет цели и задачи защиты информации
1 уровень стратегический
2 уровень оперативный
3 уровень тактический
Инструкция
Руководство
Технические регламенты

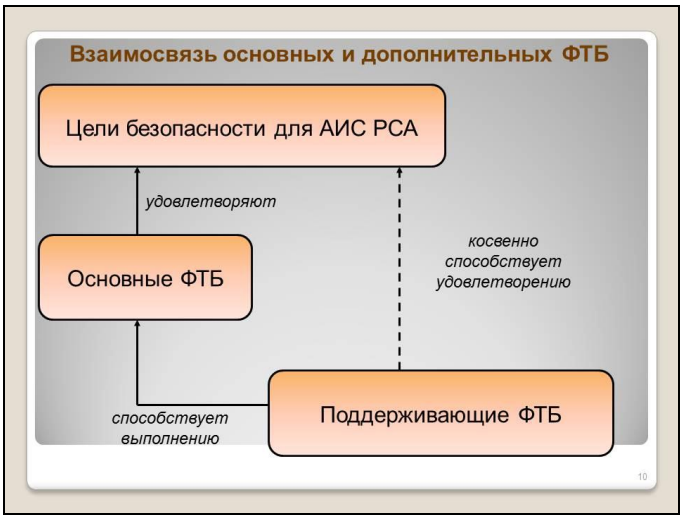

Определение общих положений Концепции
Уяснение основных направлений обеспечения безопасности информации и описание требований к безопасности информации
Разработка специальных глав Концепции
Разработка
Концепции безопасности информации

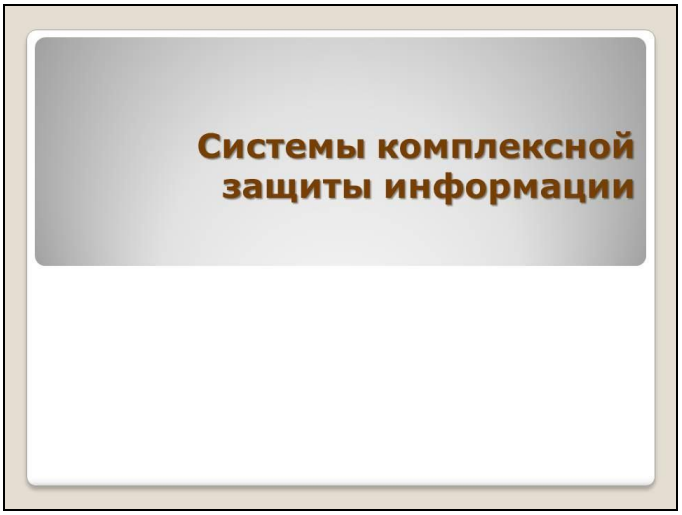

Подготовка к разработке Регламента
Определение общих положений Регламента
Определение обязанностей персонала по обеспечению безопасности информации
Определение правил использования компьютеров и информационных систем
Разработка Регламента
обеспечения безопасности информации


Разделы Профиля защиты:
✓ «Введение ПЗ»;
✓ «Описание Объекта Оценки»;
✓ «Среда безопасности ОО»;
✓ «Цели безопасности»;
✓ «Требования безопасности ИТ»;
✓ «Обоснование».


Формулировка необходимости ИБ
Описание среды, в которой находится КИС
Описание предположений о существующем состоянии безопасности
Описание политики безопасности, которая должна выполняться
Описание целей безопасности
Функциональные требования к безопасности и требования доверия к безопасности
Обоснование достаточности функциональных требований и требований доверия к безопасности
Профиль защиты включает:

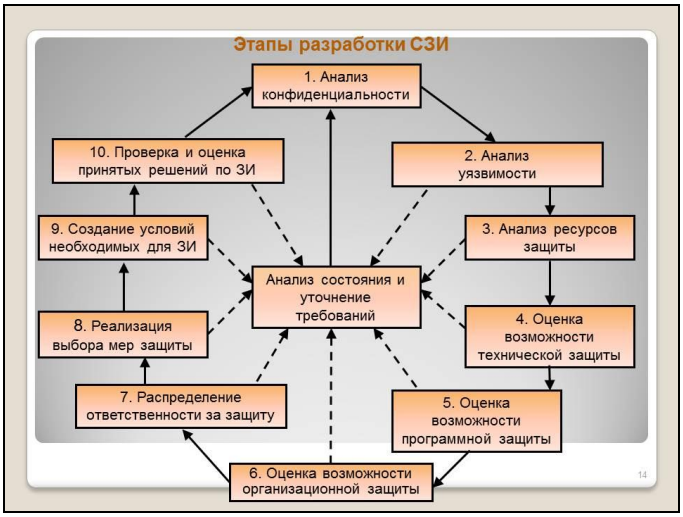

АСПЕКТЫ СРЕДЫ БЕЗОПАСНОСТИ АИС
Угрозы
Политика безопасности
Предположения безопасности
Цели безопасности
Для АИС
Для среды функционирования
Для АИС
Для среды функционирования
Не ИТ-требования безопасности
Требования безопасности к СОБИ


Взаимосвязь основных и дополнительных ФТБ
Цели безопасности для АИС РСА
удовлетворяют
Основные ФТБ
косвенно способствует удовлетворению
способствует выполнению
Поддерживающие ФТБ
10


Системы комплексной защиты информации

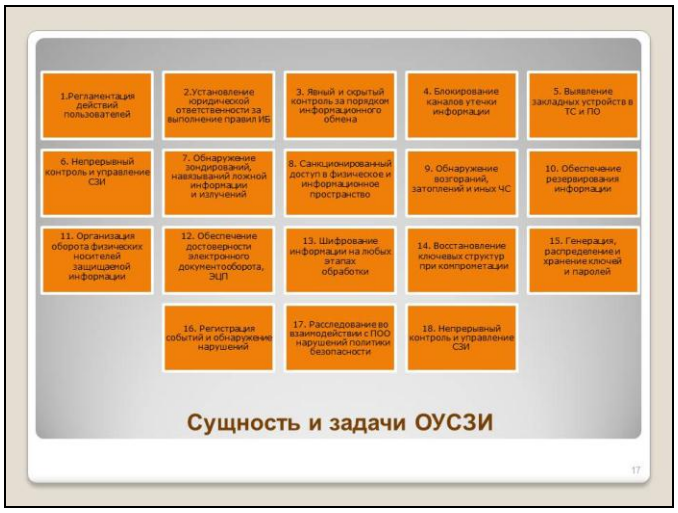

Организация системы защиты информации
Составные части
1
2
3
4
Законодательная, нормативно-методическая и научная база
Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации
Организационно-технические и режимные меры
Программно-технические методы и средства защиты информации
12


Основные направления
в общей проблеме обеспечения безопасности
1 Защита обмена ИС
2 Защита процессов и процедур обработки
3 Защита каналов связи
4 Подавление ПЭМИ
5 Управление защитой


Этапы разработки СЗИ
1. Анализ конфиденциальности
2. Анализ уязвимости
3. Анализ ресурсов защиты
4. Оценка возможности технической защиты
5. Оценка возможности программной защиты
6. Оценка возможности организационной защиты
7. Распределение ответственности за защиту
8. Реализация выбора мер защиты
9. Создание условий необходимых для ЗИ
10. Проверка и оценка принятых решений по ЗИ
Анализ состояния и уточнение требований


Параллельная разработка ИС и СЗИ
Системный подход к построению защищенных ИС
Многоуровневая структура СЗИ
Иерархическая система управления СЗИ
Блочная архитектура защищенных ИС
Возможность развития СЗИ
Дружественный интерфейс пользователя
Концепция создания защищенных ИС


Многоуровневая структура СЗИ
Для отдельного объекта можно выделить
6-7 уровней (рубежей) защиты:
Информация
Уровни защиты
1. охрана по периметру территории объекта;
2. охрана по периметру здания;
3. охрана помещения;
4. защита аппаратных средств;
5. защита программных средств;
6. защита информации.


1.Регламентация действий пользователей
2.Установление юридической ответственности за выполнение правил ИБ
3. Явный и скрытый контроль за порядком информационного обмена
4. Блокирование каналов утечки информации
5. Выявление закладных устройств в ТС и ПО
6. Непрерывный контроль и управление СЗИ
7. Обнаружение зондирований, навязываний ложной информации и излучений
8. Санкционированный доступ в физическое и информационное пространство
9. Обнаружение возгораний, затоплений и иных ЧС
10. Обеспечение резервирования информации
11. Организация оборота физических носителей защищаемой информации
12. Обеспечение достоверности электронного документооборота, ЭЦП
13. Шифрование информации на любых этапах обработки
14. Восстановление ключевых структур при компрометации
15. Генерация, распределение и хранение ключей и паролей
16. Регистрация событий и обнаружение нарушений
17. Расследование во взаимодействии с ПОО нарушений политики безопасности
18. Непрерывный контроль и управление СЗИ
Сущность и задачи ОУСЗИ


Стратегии организации защиты информации
Стратегия – общая направленность в организации деятельности с учетом объективных потребностей, возможных условий осуществления и возможностей предприятия.
Виды стратегий
Оборонительная
защита от уже известных угроз, осуществляемая автономно, без влияния на существующую ИС
Наступательная
защита от всего множества потенциальных угроз
Упреждающая
создание информационной среды, в которой угрозы не имеют условий для возникновения

Основные характеристики стратегий организации защиты информации

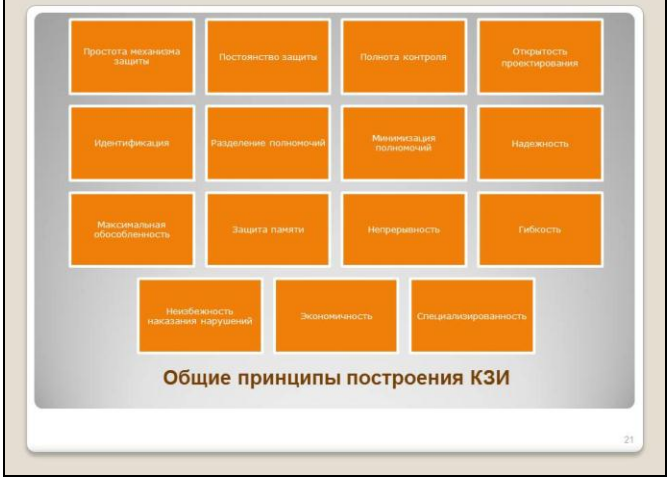
Наименование характеристики	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Возможный уровень защиты	Достаточно высок, но только в отношении известных угроз	Очень высок, но только в пределах существующих представлений о природе угроз и возможностях их проявления	Уровень защиты гарантированно очень высок
Необходимые условия реализации	Наличие методов и средств реализации	1. Наличие перечня и характеристик полного множества потенциально возможных угроз 2. Развитый арсенал методов и средств защиты 3. Возможность влиять на архитектуру ИС и технологию обработки информации	Наличие защищенных информационных технологий
Ресурсоемкость	Незначительная по сравнению с другими стратегиями	Значительная (с ростом требований по защите растет по экспоненте)	1. Высокая в плане капитальных затрат 2. Незначительная в каждом конкретном случае при наличии унифицированной защищенной ИТ
Рекомендации по применению	Невысокая степень секретности защищаемой информации и не очень большие ожидаемые потери	Достаточно высокая степень секретности защищаемой информации и возможность значительных потерь при нарушении защиты	Перспективная

19

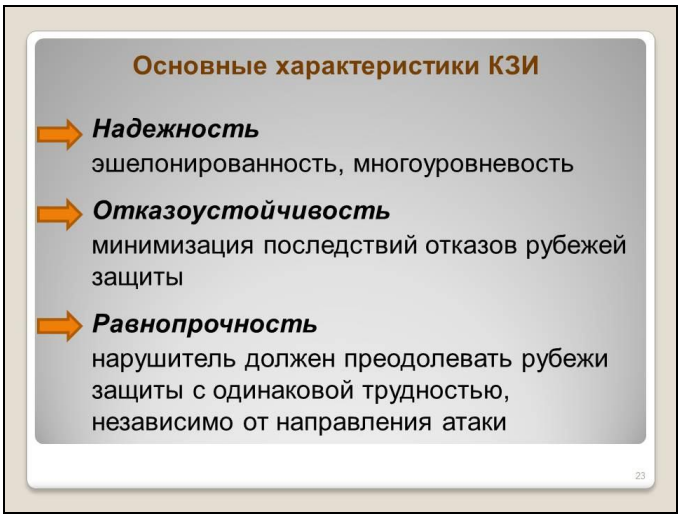
Этапы построения СЗИ для различных стратегий

Наименование этапов построения	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Формирование среды защиты		1. Структурированная архитектура ИС 2. Структурированная технология обработки ЗИ 3. Четкая организация работ по защите	Защищенная информационная технология в унифицированном исполнении
Анализ средств защиты	1. Представление организационной структуры ИС в виде графа, узлы – типовые структурные компоненты, а дуги – взаимосвязи между компонентами 2. Представление технологии обработки ЗИ в виде строго определенной схемы 3. Определение параметров ЗИ и условий ее обработки		
Оценка уязвимости информации	1. Определение значений вероятности нарушения защиты информации в условиях ее обработки 2. Оценка размеров возможного ущерба при нарушении защиты		
Определение требований к защите	Определение вероятности нарушения защиты информации, которая должна быть обеспечена при обработке защищаемой информации		
Построение системы комплексной защиты	Определение технических средств, которые должны быть использованы при обработке ЗИ	Выбор типового варианта или проектирование индивидуальной системы КЗИ	Определение механизмов защиты, которые должны быть задействованы при создании КЗИ
Требования к среде защиты		Определяется в зависимости от требований к защите информации	Реализуется на базе унифицированной защищенной ИТ

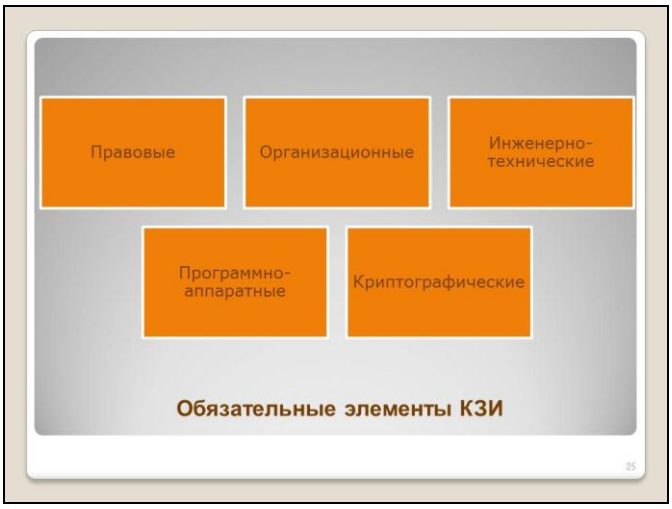
20

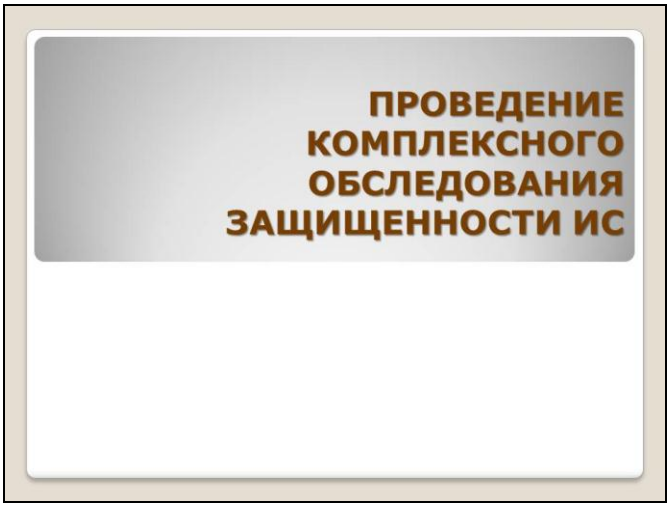


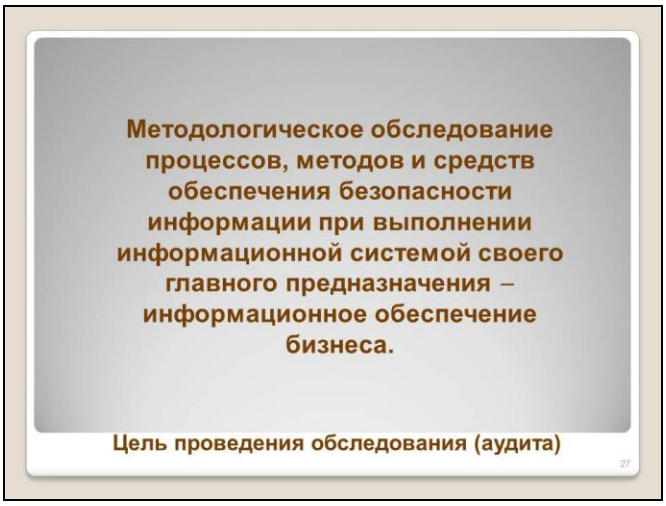

Структура КЗИ
Информация
Документ
Режим
Программа
Аппарат
Охрана
Техника
Инженерные сооружения
22


Основные характеристики КЗИ
Надежность
эшелонированность, многоуровневость
Отказоустойчивость
минимизация последствий отказов рубежей защиты
Равнопрочность
нарушитель должен преодолевать рубежи защиты с одинаковой трудностью, независимо от направления атаки
23


Этапы разработки КЗИ
I. Определение информации, подлежащей защите
II. Выявление полного множества угроз и критериев утечки информации
III. Проведение оценки уязвимости и рисков информации по имеющимся угрозам и каналам утечки
IV. Определение требований к комплексной защите
V.Осуществление выбора средств защиты информации и их характеристик
VI. Внедрение и организация использования выбранных мер, способов и средств защиты
VII.Осуществление контроля целостности и управление системой защиты
Постоянный анализ и уточнение требований к КЗИ


Правовые
Организационные
Инженерно-технические
Программно-аппаратные
Криптографические
Обязательные элементы КЗИ


ПРОВЕДЕНИЕ КОМПЛЕКСНОГО ОБСЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ ИС


Методологическое обследование процессов, методов и средств обеспечения безопасности информации при выполнении информационной системой своего главного предназначения – информационное обеспечение бизнеса.
Цель проведения обследования (аудита)

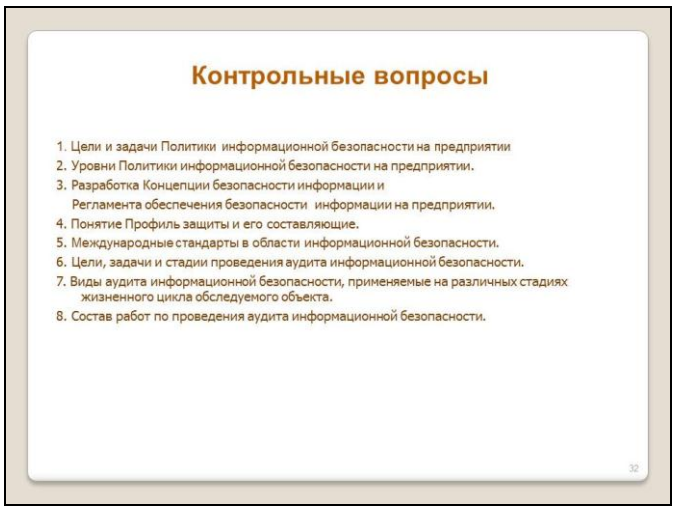


Виды обследования

Периоды жизненного цикла обследуемого объекта	Виды обследования (аудита)				
	Первичный	Технический	Аттестация	Сертиф.	Контрольный
Принятие решения о создании корпоративной ИС	x				
Определение требований к создаваемой корпоративной ИС		x			
Проектирование и ввод в эксплуатацию корпоративной ИС			x	x	
Штатная эксплуатация средств корпоративной ИС					x
Ремонт (плановый и внеплановый), устранение неисправностей			x		x
Нештатные ситуации, приводящие к ущербу				x	x
Устранение последствий нештатных ситуаций					x
Принятие решений о модернизации корпоративной ИС	x	x	x		
Модернизация корпоративной ИС				x	
Эксплуатация модернизированной ИС					x
Вывод из эксплуатации и замена корпоративной ИС					x







Литература: Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637

Лекция 7. Инструментальные средства аудита ИБ

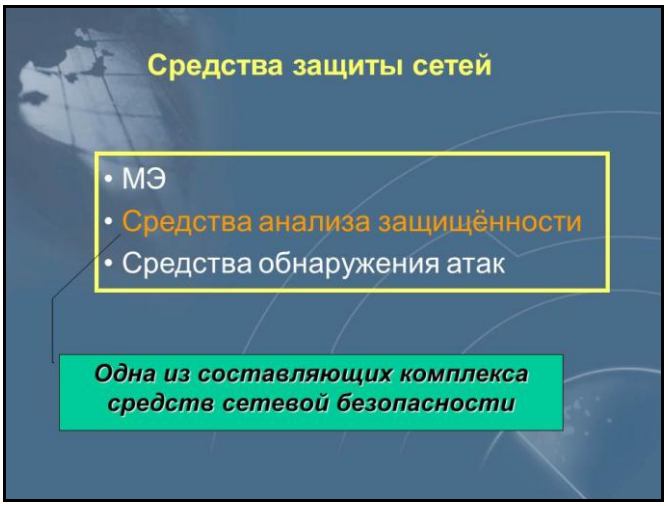
Тезисы лекции:

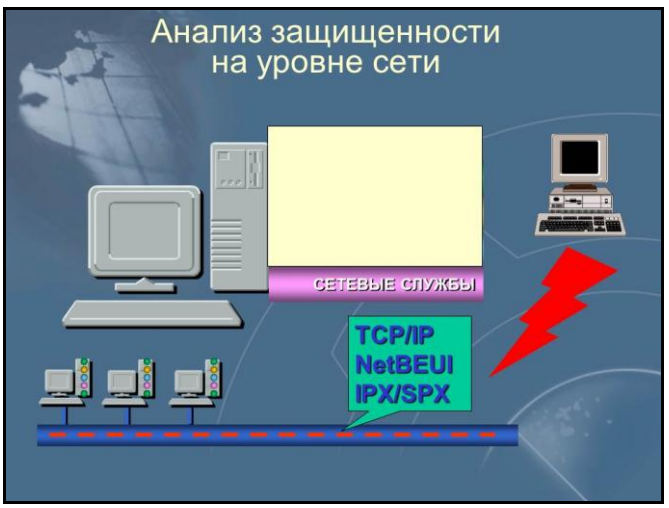
- Методы и инструментальные средства проведения активного аудита ИБ.
- Обнаружение и устранение уязвимостей. Возможности сканеров безопасности, мониторинг событий безопасности. Классификация и архитектура сканеров безопасности. Схемы подключения сканеров безопасности. Основные этапы работы сканеров безопасности. Особенности проведения сканирования корпоративных вычислительных сетей. Внедрение сканеров безопасности в корпоративной сети.
- Подключение сетевых средств защиты с высокой доступностью. Общие требования и особенности. Методы сбора информации о сети.
- Методы идентификация устройств в сети и их реализация в сканерах безопасности.
- Пассивный анализ информационных потоков.
- Методы идентификация открытых портов и их реализация в сканерах безопасности.

- Методы идентификация служб и приложений узла и их реализация в сканерах безопасности.

Слайды презентации к лекции:







Средства анализа защищённости

	Net Recon	HackerShield	Retina	Internet Scanner	Nessus Security Scanner	CyberCop Scanner	SARA	SAINT
Производитель	Axent Technologies	BindView	eEye Digital Security	Internet Security Systems		Network Associations		WW Digital Security
Платформа	Windows NT	Windows NT	Windows NT	Windows NT Workstation	Unix	Windows NT	Unix	Unix
Возможность обновления	+	+	+	+	+	+	-	-
Возможность создания собственных проверок	-	-	-	-	+	+	+	+

Средства анализа защищённости

	Net Recon	HackerShield	Retina	Internet Scanner	Nessus Security Scanner	CyberCop Scanner	SARA	SAINT
Работа из командной строки	-	-	-	+	+	+	+	+
Поддержка CVE	-	+	-	+	+	-	+	+
Автоматическое устранение уязвимостей	-	+	+	-	-	+	-	-
Открытость кода	-	-	-	-	+	-	+	+
Коммерческий или бесплатный	+	+	+	+	-	+	-	-
Интерфейс (по пятибалльной шкале)	4,5	4	4	4,5	3	4,5	2	2
Отчеты (по пятибалльной шкале)	3,5	2	2	3,5	3,5	3	2	2

Этапы анализа защищенности на уровне сети

Сбор информации о сети

Категорирование сетевых устройств

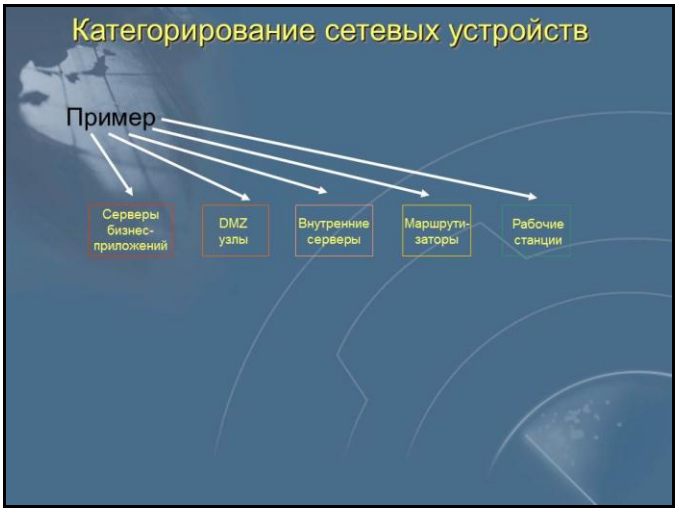
Выбор объектов сканирования и вариантов размещения сканера (сканеров)

Выбор (разработка) политик сканирования

Составление расписания сканирования

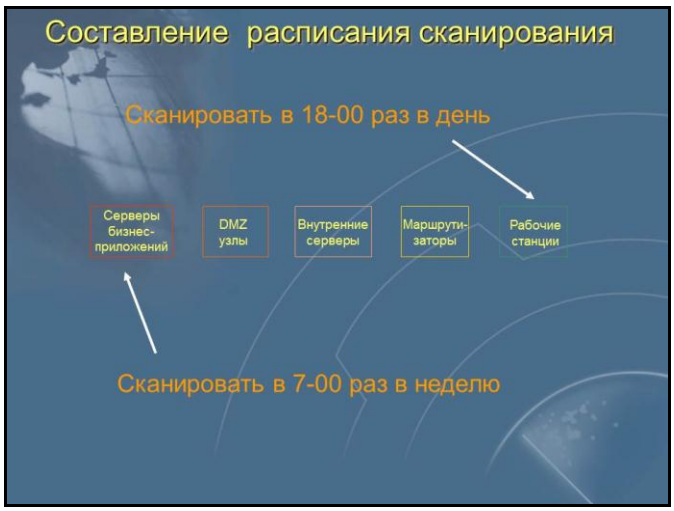
Сканирование и анализ результатов


Сбор информации о сети
Филиал
DMZ-1
МЭ
Мобильные сотрудники
DMZ-2
Ресурсы Internet
Пользователи Internet


Категорирование сетевых устройств
Пример
Серверы бизнес-приложений
DMZ узлы
Внутренние серверы
Маршрути-заторы
Рабочие станции

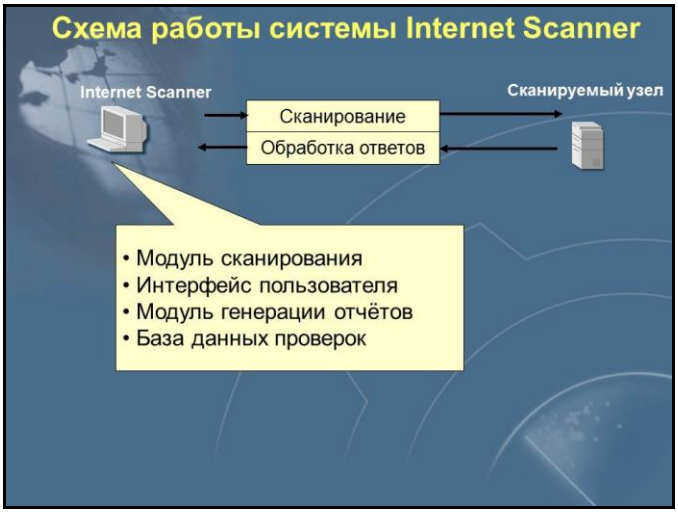

Выбор объектов сканирования и вариантов расположения средств анализа защищённости
Корпоративная сеть
Human Resources
Marketing
Engineering
manufacturing
DMZ
E-mail
File Transfer
HTTP
Firewall
Router
Internet


Выбор политик сканирования
Политика для рабочих станций
Серверы бизнес-приложений
DMZ узлы
Внутренние серверы
Маршрути-заторы
Рабочие станции
Политика для критичных узлов
(максимальная защита)


Составление расписания сканирования
Сканировать в 18-00 раз в день
Серверы бизнес-приложений
DMZ узлы
Внутренние серверы
Маршрути-заторы
Рабочие станции
Сканировать в 7-00 раз в неделю


Сканирование и анализ результатов
Филиал
Отчет о сканировании
Мобильные сотрудники
Ресурсы Internet
Пользователи Internet

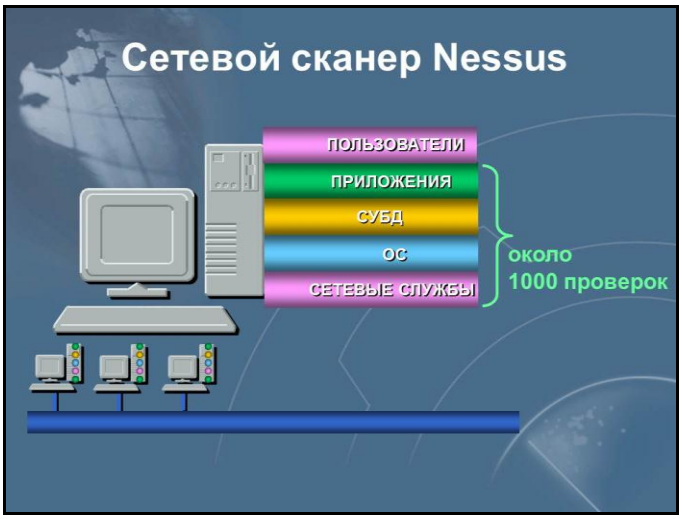

Internet Scanner
(пример сканера сетевого уровня)


Схема работы системы Internet Scanner
Internet Scanner
Сканируемый узел
Сканирование
Обработка ответов
• Модуль сканирования
• Интерфейс пользователя
• Модуль генерации отчётов
• База данных проверок

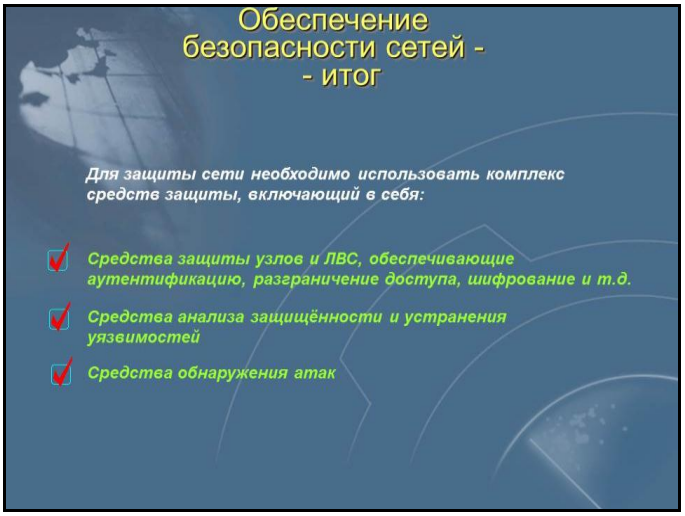

Уровни сканирования
Level 1
Типы операционных систем узлов
Level 2
Запущенные на узлах службы
Level 3
Возможность атак со стороны неквалифицированных злоумышленников
Level 4
Возможность атак с помощью различных инструментальных средств
Level 5
Высокая квалификация атакующего, проверка неверных конфигураций
Рабочие станции
Серверы бизнес-приложений


Категории отчетов
• Для руководства компании
• Для руководителей отделов
• Для технических специалистов
Итоговый отчет по уязвимостям
Общее число уязвимостей
Уязвимости по степени риска (в %)
High
Medium
Low


Сетевой сканер Nessus
Nessus-клиент (Windows, UNIX)
Nessus-сервер (UNIX)
Сканируемая сеть


Сетевой сканер Nessus
ПОЛЬЗОВАТЕЛИ
ПРИЛОЖЕНИЯ
СУБД
ОС
СЕТЕВЫЕ СЛУЖБЫ
около
1000 проверок


Параллельное подключение и сканирование
Nessus-клиент
Nessus-клиент
Nessus-сервер (UNIX)
Сканируемая сеть
Nessus-клиент


Обеспечение безопасности сетей - - итог
Для защиты сети необходимо использовать комплекс средств защиты, включающий в себя:
Средства защиты узлов и ЛВС, обеспечивающие аутентификацию, разграничение доступа, шифрование и т.д.
Средства анализа защищённости и устранения уязвимостей
Средства обнаружения атак


Средства защиты периметра
Филиал
DMZ-1
МЭ
Internet
Мобильные сотрудники
DMZ-2
Рабочие места
Ресурсы Internet
Пользователи Internet





Литература: Веселов, Г. Е. Менеджмент риска информационной безопасности : учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 109 с. : схем., табл. - Библиогр.: с.85-86 - ISBN 978-5-9275-2327-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493331

Лекция 8. Изучение практического опыта технического аудита безопасности АИС предприятий

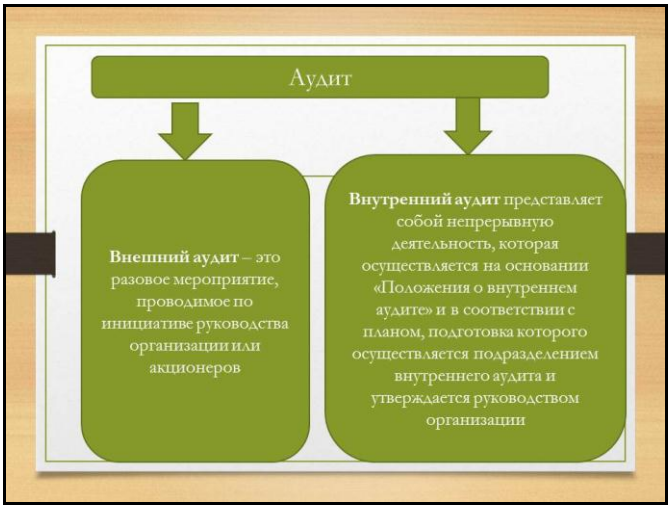
Тезисы лекции:

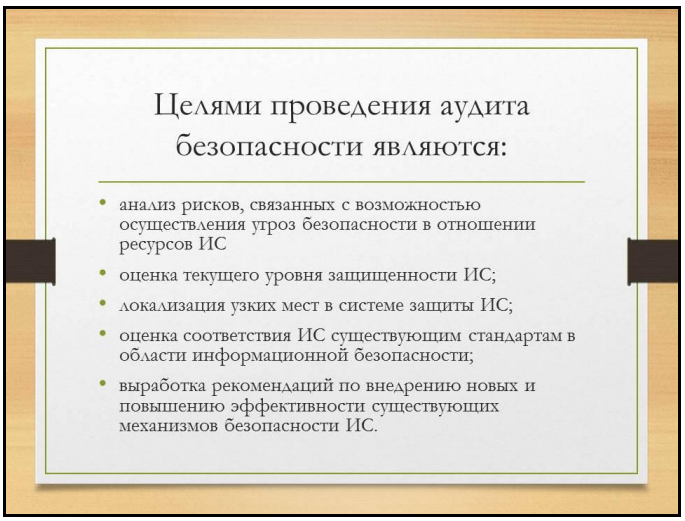
- Анализ опыта и рекомендации по планированию: инициирование процедуры аудита, цель планирования, объект обследования, порядок планирования аудита, анализ значимости информационных ресурсов, анализ процесса обработки информации, отчетные материалы, условия соблюдения конфиденциальности.
- Анализ опыта и рекомендации по моделированию: цель моделирования, методы обследования на этапе моделирования, порядок проведения моделирования, отчетные материалы.
- Анализ опыта и рекомендации по тестированию: цель, методы и порядок проведения тестирования, проверка реальных условий размещения и использования оборудования, тестовые испытания функций защиты от НСД и защиты от утечки по техническим каналам, отчетные материалы.
- Анализ опыта и рекомендации по анализу и документированию результатов: цель и методы обследования на этапе анализа, анализ организационно-распорядительных

документов, выполнения организационно-технических требований, деятельности персонала (сотрудников), отчетные материалы, рекомендации по документированию результатов: цель документирования.

Слайды презентации к лекции:

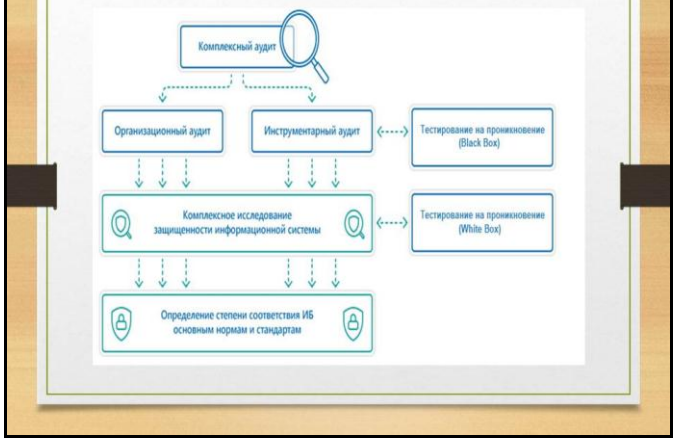






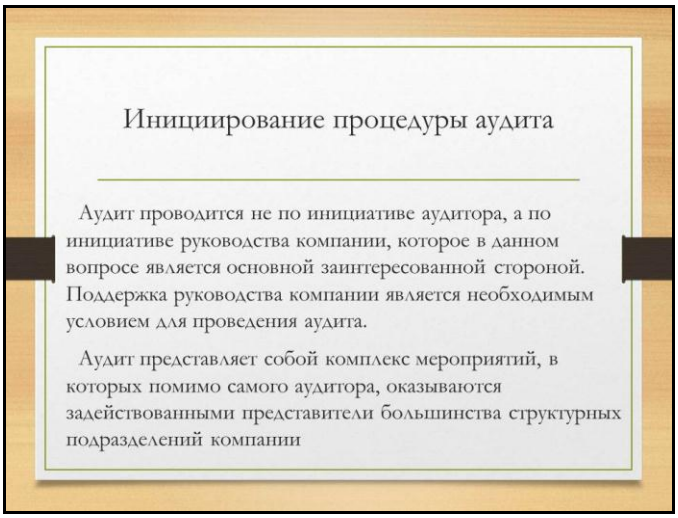
Дополнительные задачи внутренних аудиторов:

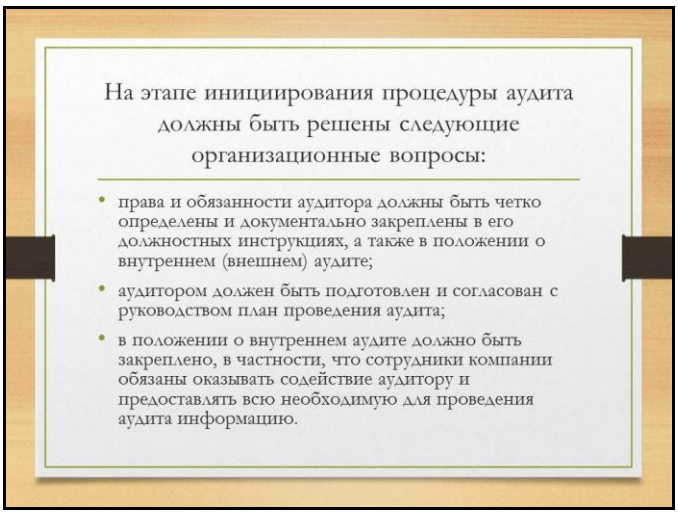
- участие в их внедрении в работу организации;
- постановка задач для ИТ персонала, касающихся обеспечения защиты информации;
- участие в обучении пользователей и обслуживающего персонала ИС вопросам обеспечения информационной безопасности;
- участие в разборе инцидентов, связанных с нарушением информационной безопасности;



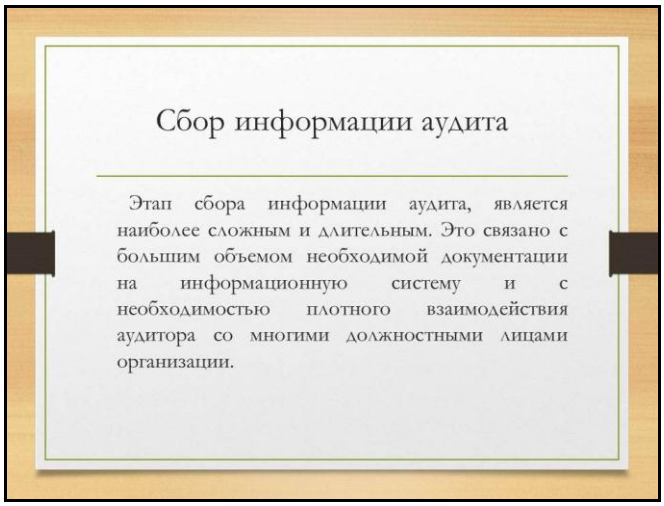
Этапность работ по проведению аудита безопасности информационных систем

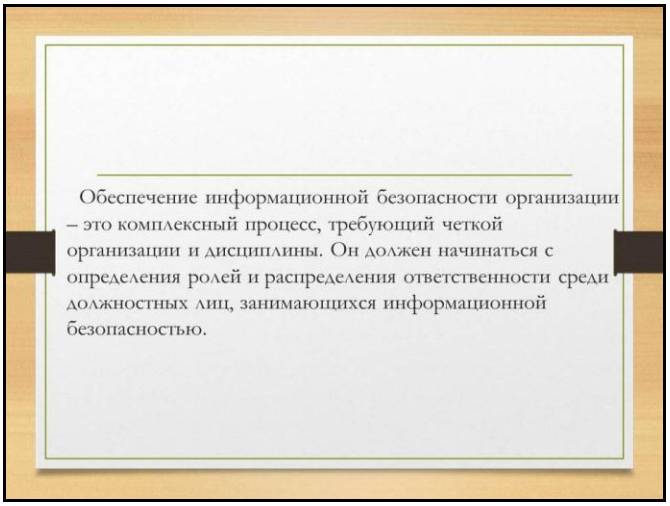
- Инициирование процедуры аудита
- Сбор информации аудита
- Анализ данных аудита
- Выработка рекомендаций
- Подготовка аудиторского отчета

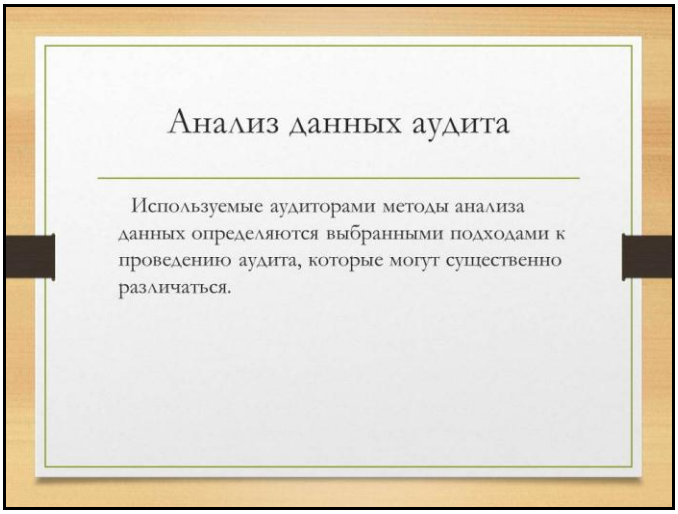

Инициирование процедуры аудита
Аудит проводится не по инициативе аудитора, а по инициативе руководства компании, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства компании является необходимым условием для проведения аудита.
Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора, оказываются задействованными представители большинства структурных подразделений компании

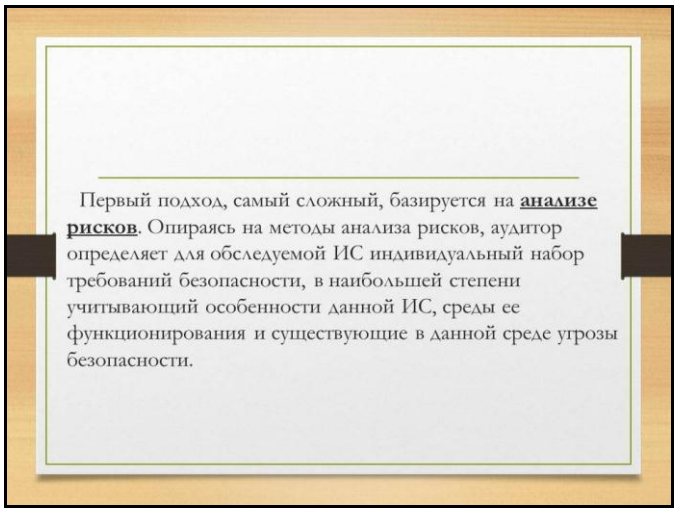

На этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы:
права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;
аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники компании обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

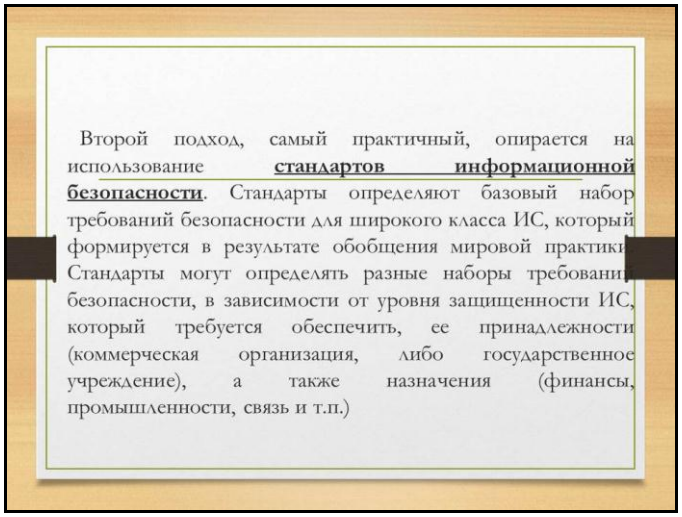

Границы проведения обследования определяются в следующих терминах:
Список обследуемых физических, программных и информационных ресурсов;
Площадки (помещения), попадающие в границы обследования;
Основные виды утроз безопасности, рассматриваемые при проведении аудита;
Организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты (в каком объеме они должны быть учтены).

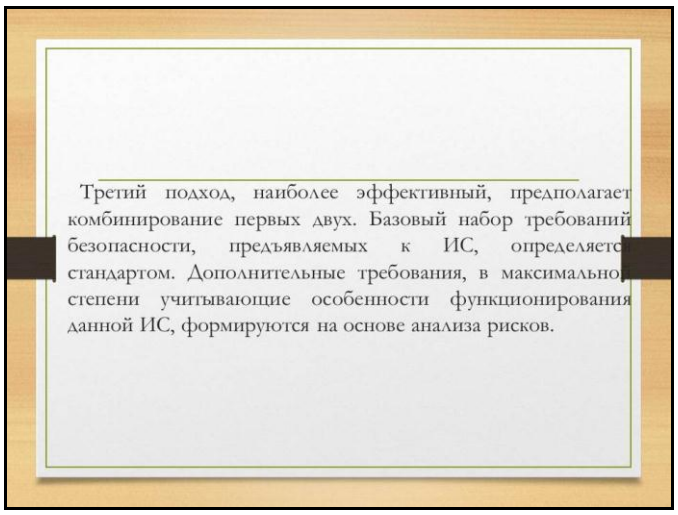

Сбор информации аудита
Этап сбора информации аудита, является наиболее сложным и длительным. Это связано с большим объемом необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

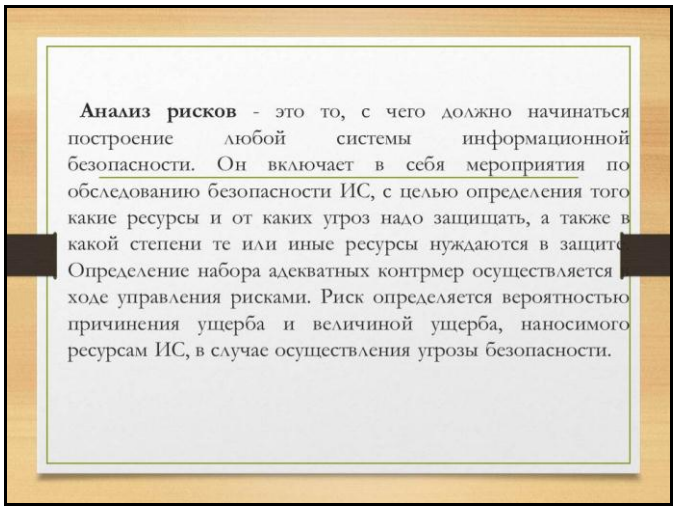

Обеспечение информационной безопасности организации – это комплексный процесс, требующий четкой организации и дисциплины. Он должен начинаться с определения ролей и распределения ответственности среди должностных лиц, занимающихся информационной безопасностью.

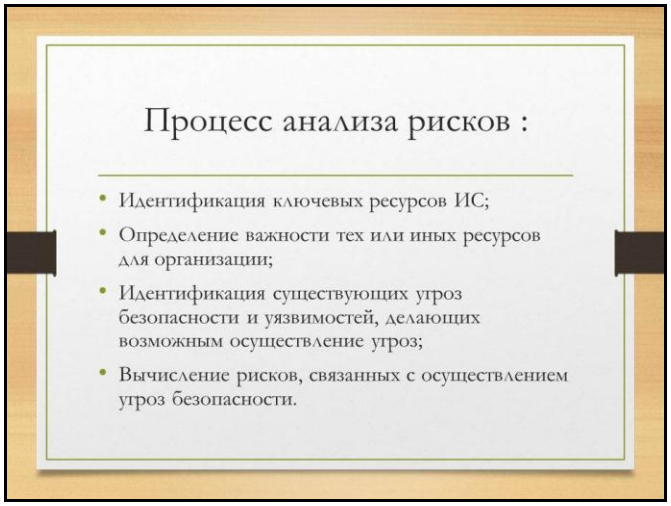

Анализ данных аудита
Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

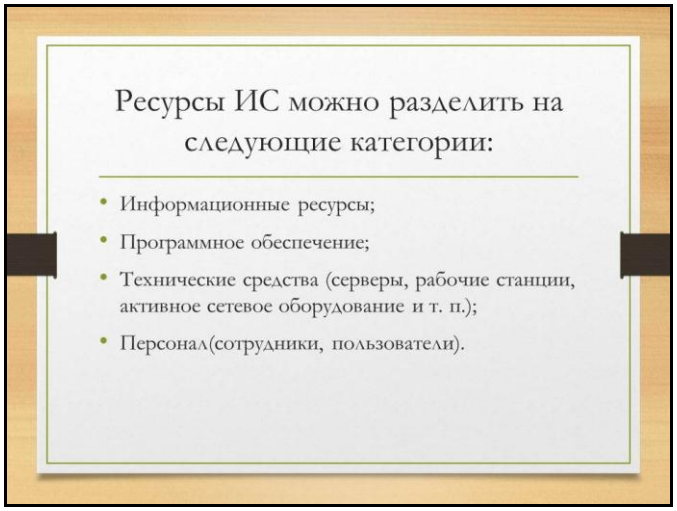

Первый подход, самый сложный, базируется на **анализе рисков**. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности.

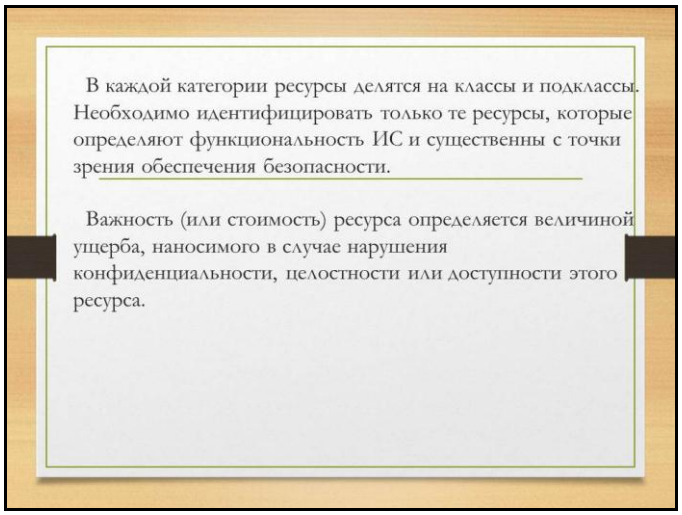

Второй подход, самый практичный, опирается на использование **стандартов информационной безопасности**. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т.п.)

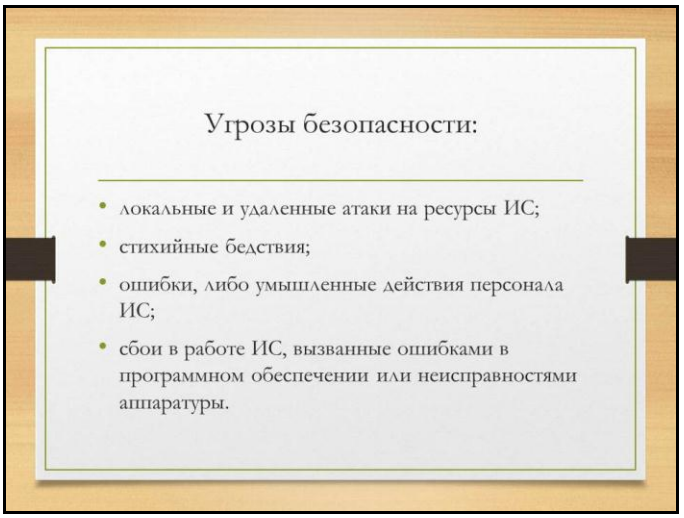

Третий подход, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков.

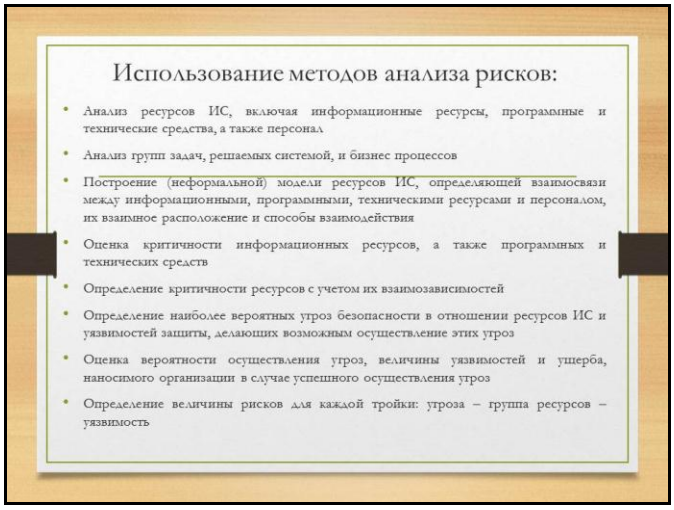

Анализ рисков - это то, с чего должно начинаться построение любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности.

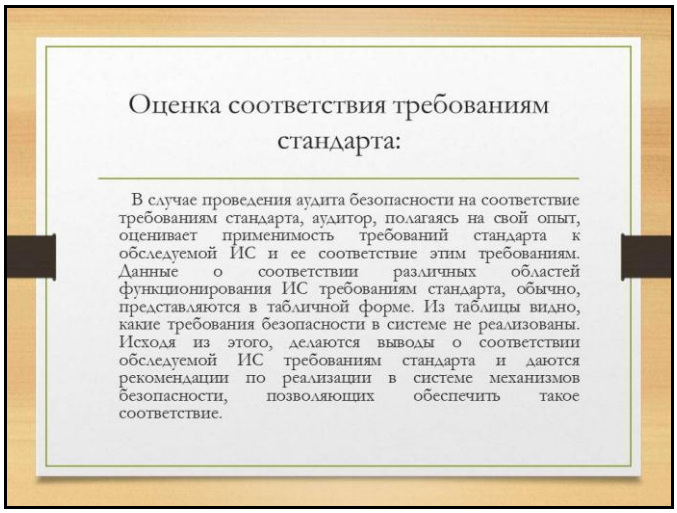

Процесс анализа рисков :
Идентификация ключевых ресурсов ИС;
Определение важности тех или иных ресурсов для организации;
Идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз;
Вычисление рисков, связанных с осуществлением угроз безопасности.

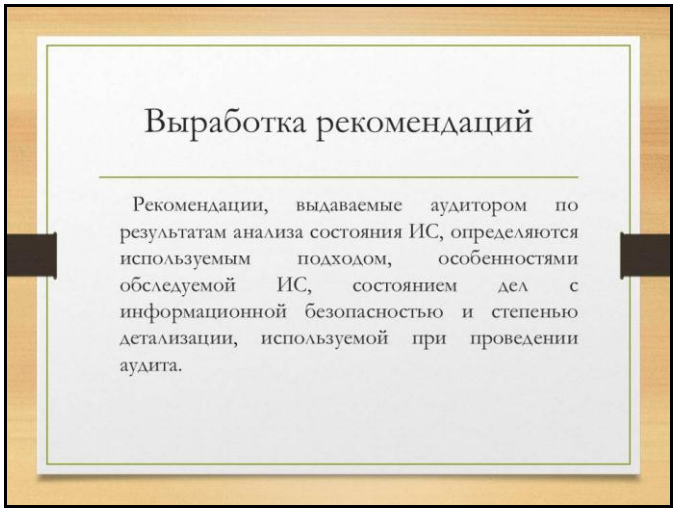

Ресурсы ИС можно разделить на следующие категории:
Информационные ресурсы;
Программное обеспечение;
Технические средства (серверы, рабочие станции, активное сетевое оборудование и т. п.);
Персонал(сотрудники, пользователи).

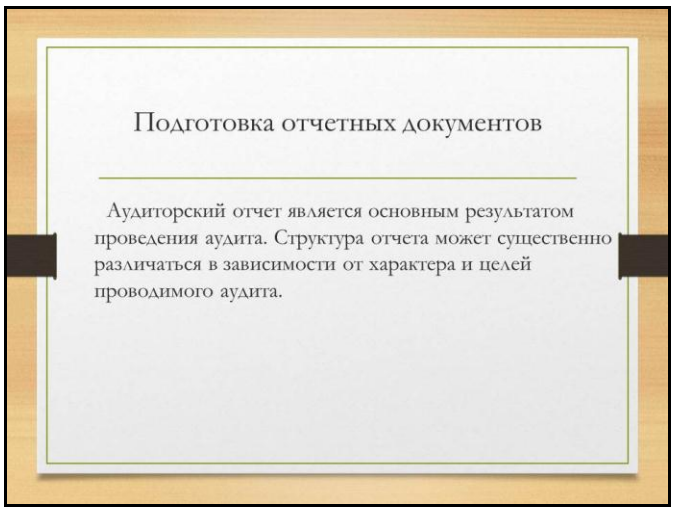

В каждой категории ресурсы делятся на классы и подклассы. Необходимо идентифицировать только те ресурсы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности.
Важность (или стоимость) ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса.

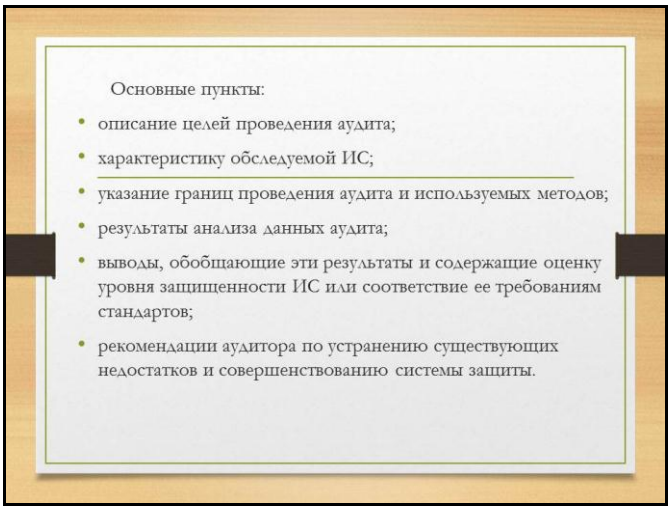

Угрозы безопасности:
локальные и удаленные атаки на ресурсы ИС;
стихийные бедствия;
ошибки, либо умышленные действия персонала ИС;
сбои в работе ИС, вызванные ошибками в программном обеспечении или неисправностями аппаратуры.


Использование методов анализа рисков:
Анализ ресурсов ИС, включая информационные ресурсы, программные и технические средства, а также персонал
Анализ групп задач, решаемых системой, и бизнес процессов
Построение (неформальной) модели ресурсов ИС, определяющей взаимосвязи между информационными, программными, техническими ресурсами и персоналом, их взаимное расположение и способы взаимодействия
Оценка критичности информационных ресурсов, а также программных и технических средств
Определение критичности ресурсов с учетом их взаимозависимостей
Определение наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз
Оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз
Определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость


Оценка соответствия требованиям стандарта:
В случае проведения аудита безопасности на соответствие требованиям стандарта, аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой ИС и ее соответствие этим требованиям. Данные о соответствии различных областей функционирования ИС требованиям стандарта, обычно, представляются в табличной форме. Из таблицы видно, какие требования безопасности в системе не реализованы. Исходя из этого, делаются выводы о соответствии обследуемой ИС требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.


Выработка рекомендаций
Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита.


Подготовка отчетных документов
Аудиторский отчет является основным результатом проведения аудита. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита.



Литература: Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 100 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1277-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93259

Лекция 9. Итоговая лекция. Подведение и анализ промежуточных результатов освоения дисциплины

Итоговая лекция завершает изучение дисциплины, обобщает пройденное за весь период. При ее подготовке учитываются пробелы в знаниях аспирантов, выявленные на практических занятиях и при оценке самостоятельной работы. Аспиранты получают установку на их устранение и на дальнейшее совершенствование своей подготовки в данной области. На лекции подводятся итоги изучения дисциплины, показывается ее значение в профессиональной сфере и формировании научного мировоззрения, обсуждается вопрос о подведении итогов изучения дисциплины – сдаче зачета или экзамена.

2. Методические указания по подготовке к занятиям семинарского типа

2.1. Планы и (или) методические рекомендации к практическим занятиям

В рамках проведения занятий по дисциплине предполагается организация следующих практических занятий:

Практическое занятие 1. Общие сведения о безопасности компьютерных систем, проведении ее анализа

Тематика: Термины и определения.

Текст задания:

а) Выбрать любые три темы из данного списка. Представить основные моменты выбранных тем в виде презентации.

1. Понятие кибертерроризма.
2. Понятие кибершпионажа.
3. Атаки на государственные ИС и ИС критически важных объектов.
4. Понятие информационной войны.
5. История информационных войн.
6. Основные черты и особенности информационной войны.
7. Модели и методы ведения информационной войны.

8. Информационное оружие. Виды и функции.
9. Возможные объекты нападения с применением информационного оружия.
10. Основы информационного противоборства.
11. Основы информационно-психологического воздействия. Основные каналы информационно-психологического воздействия.
12. Основы противодействия информационному воздействию.
13. Методы и средства информационно-психологического воздействия.
14. Угрозы информационно-психологического воздействия для личности, общества, государства.
15. Основные документы Российской Федерации и зарубежных стран в области противодействия угрозам национальной информационной безопасности: кибертерроризму и кибер- и информационным войнам, а также в области противодействия информационному воздействию.

б) Найти определения следующих понятий:

- фишинг;
- сниффинг пакетов в локальной сети;
- IP-спуфинг;
- DDos (Denial of Service);
- XSS (Cross-Site Scripting);
- SQL-Injection;
- Mail-bombing;
- CSRF (Cross Site Request Forgery);
- Dummy DNS Server;
- DNS Cache Poisoning (Атака Каминского).

Шкала оценивания:
Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;
Оценка «хорошо» выставляется, если при создании презентации аспирант недостаточно полно представил выбранные темы, ошибки или неточности в определениях отсутствуют;
Оценка «удовлетворительно» выставляется, если в сформулированных определениях присутствуют ошибки.
Оценка «неудовлетворительно» выставляется, если аспирант не выполнил или выполнил работу не полностью.

Практическое занятие 2. Содержание работ при аудите безопасности информационных систем

Тематика: Стадии аудита: моделирование.
Практическая работа, включенная в методические указания, призвана помочь понять, как на практике необходимо строить описание программного обеспечения в виде диаграмм потоков данных и определять угрозы безопасности информации, возникающие вследствие применения программного обеспечения по методике STRIDE.

Текст задания: Выберите один из предложенных ниже типов программных продуктов. Постройте диаграмму потоков данных для выбранного продукта. Идентифицируйте угрозы, которые могут возникнуть вследствие его применения. Предложите противодействия по каждой угрозе.

Программные продукты:
1. Система управления предприятием.
2. Средство антивирусной защиты с централизованным управлением.
3. Система контейнеризации.
4. Система сбора логов.
5. Система централизованного обновления машин.
6. Система биометрической идентификации.
7. Система сбора и расчета аналитики.
8. Система распределенного контроля версий.
9. Система централизованного контроля версий.
10. Гипервизор (1-го или 2-го типа).

Для построения диаграммы потоков данных рекомендуется использовать библиотеку threatmodeling для продукта Draw.io. Для использования выполните следующие шаги:

11. Скачайте и установите Draw.io по ссылке https://about.draw.io/integrations/#integrations_offline
12. Клонируйте репозиторий https://github.com/michenriksen/drawio-threatmodeling
13. В Draw.io создайте новую диаграмму
14. Нажмите «Файл (File)» – «Открыть библиотеку (Open library)». Выберите XML файл из клонированного проекта.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если работа выполнена полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 3. Методология проведения аудита информационной безопасности

Тематика: Методы и средства анализа защищенности.

Постановка задачи:

В соответствии с заданием требуется проанализировать трафик, захваченный программой *Wireshark,* а именно:

1) рассмотреть структуру пакета, указав назначение каждого заголовка;

2) пояснить механизм инкапсуляции протоколов.

В отчете привести скриншоты, иллюстрирующие ответы на поставленные в задании вопросы (также пакет можно распечатать прямо из программы *Wireshark*). Необходимо иметь с собой на flash-носителе сохраненную версию захваченного трафика (так называемый дамп трафика) в формате pcap (это стандартный формат сохранения трафика в Wireshark).

Во всех вариантах задания необходимо выполнить следующие этапы исследования.

Протокол IP

1) запустить *Wireshark;*
2) запустить процесс захвата трафика;
3) в командной строке: tracert конечный_узел

например, tracert wireshark.org

в качестве конечного узла использовать URL, в котором по очереди встречаются инициалы фамилии и имени студента в латинской транскрипции (например, для имени Пётр Иванов подойдут адреса сайтов http://pictures.com или http://nopix.ru/;

4) остановить захват трафика.

В информационном поле разверните строку, содержащую «Internet Protocol». Ответьте на следующие вопросы.

1. Проанализируйте первый пакет ICMP Echo Request, отправленный вашим компьютером: укажите ваш IP-адрес.
2. Приведите значение поля, определяющее протокол верхнего уровня.
3. Сколько байт содержится в заголовке IP? Сколько байт в поледанных?
4. Укажите значение TTL. Как изменяется это поле в разных ICMP EchoRequest?
5. Какое значение содержится в поле «Identification»? Для чего используется это поле?

Фрагментация пакетов

1) запустить *Wireshark;*
2) запустить процесс захвата трафика;
3) в командной строке:
4) ping –l 2000 конечный_узел (ключ -l позволяет указать загрузку поля «Data» пакета в байтах)

например, ping –l 2000 wireshark.org

в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.Ответьте на следующие вопросы.

1. Проанализируйте пакет ICMP Echo Request: имеет ли место фрагментация исходного пакета, какое поле на это указывает?
2. Проанализируйте фрагменты IP-дейтаграммы: какая информация указывает, является ли фрагмент пакета последним или промежуточным?
3. Укажите количество фрагментов исходного пакета.

На этом общая часть задания заканчивается. Описание вариативной части приведено в следующем параграфе. Номер варианта выдает преподаватель.

Описание программы Wireshark

Для выполнения лабораторной работы необходимо установить на компьютер программу-анализатор сетевых пакетов Wireshark, скачав ее с официального сайта http://wireshark.org. На рис. 1 представлено главное окно *Wireshark.*

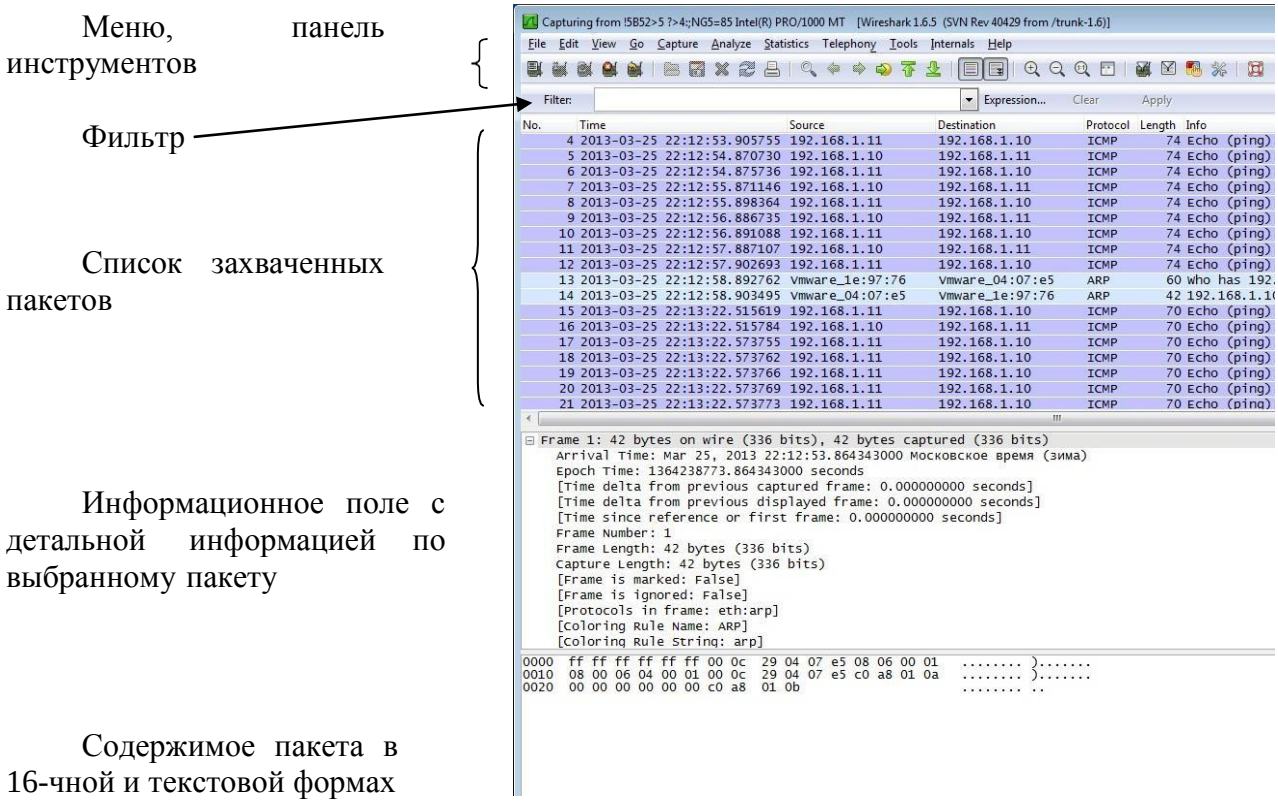


Рис. 1. Wireshark GUI

Начать работу с Wireshark следует следующим образом:

1) открыть браузер;
2) запустить *Wireshark*:
   a) установить параметры для захвата трафика; в качестве интерфейса, используемого для захвата трафика, выбратьфизический адаптер, тип адаптера — Local (рис. 2);
   b) запустить процесс захвата трафика (кнопка *Start*);
3) в браузере открыть любой сайт (например, http://www.wireshark.org/docs/wsug_html_chunked/);
4) установить значение фильтра, равным http;

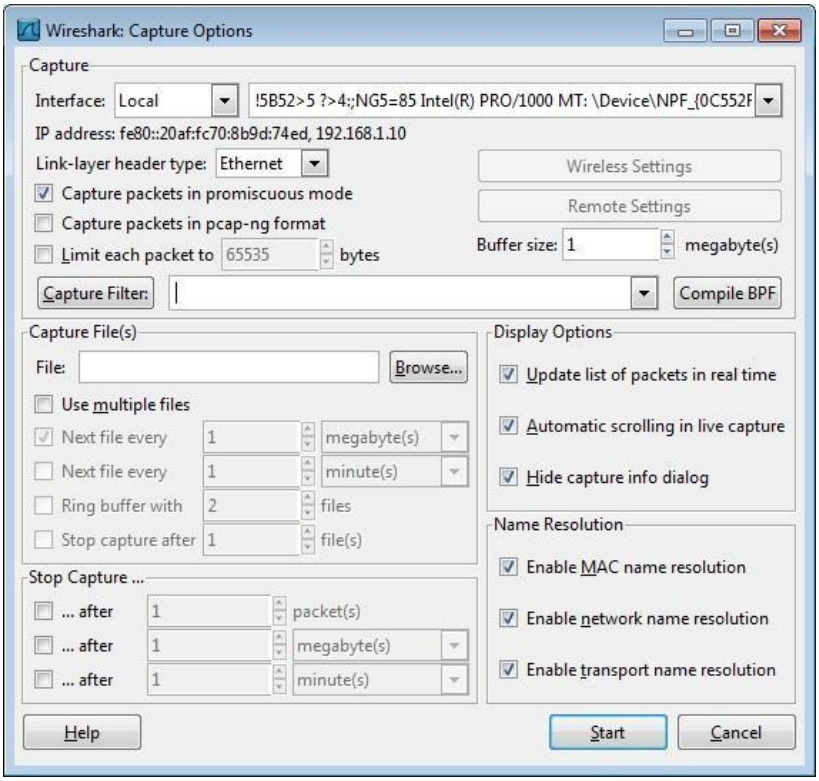


Рис. 2. Параметры захвата трафика

5) выбрать первое http сообщение в списке пакетов — это будет сообщение HTTP GET, отправленное на указанный хост (например, www.wireshark.org); в информационном поле отображена детальнаяинформация по заголовкам пакета.

Варианты задания

Вариант 1. HTTP: Basic HTTP GET/response

1) запустить *Wireshark;*

2) настроить фильтр (http);

3) запустить процесс захвата трафика;

4) URL: например, http://wiki.wireshark.org/;

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Прим.: Не принимать во внимание HTTP запрос и ответ для favicon.ico. Появление ссылки на данный файл означает, что браузер автоматически

запрашивает сервер о наличии маленького значка веб-сайта, т. н.

«Favicon» (отображается браузером в адресной строке перед URL страницы,а также в качестве картинки рядом с закладкой, во вкладках и в других элементах интерфейса).

В списке захваченных пакетов найдите пару HTTP сообщений (запрос- ответ): GET сообщение и ответ сервера.

В информационном поле разверните строку, содержащую HTTP, и отметьте указанную ниже информацию.

1. Версия HTTP.
2. Принимаемые браузером языки.
3. IP-адреса вашего компьютера и сервера.
4. Код состояния HTTP. Что он означает?
5. Длина тела сообщения. (Содержимое поля заголовка объекта Content- Length указывает длину тела сообщения в октетах (десятичное число),или в случае метода HEAD, размер тела объекта, который мог бы быть послан при запросе GET.)
6. Протокол транспортного уровня, который использует HTTP.

Вариант 2. HTTP: HTTP CONDITIONAL GET/response(Условный GET)

1) очистить кэш браузера;
2) открыть браузер;
3) запустить *Wireshark;*
4) запустить процесс захвата трафика;
5) URL: например, http://www.w3.org/Protocols/rfc2616/rfc2616- sec10.html

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

6) быстро обновить страницу в браузере;
7) остановить захват трафика;
8) настроить фильтр (http).

Прим.: Не принимать во внимание HTTP запрос и ответ для favicon.ico. Появление ссылки на данный файл означает, что браузер автоматическизапрашивает сервер о наличии маленького значка веб-сайта, т. н.

«Favicon» (отображается браузером в адресной строке перед URL страницы,а также в качестве картинки рядом с закладкой, во вкладках и в других элементах интерфейса).

Ответьте на следующие вопросы.

1. Укажите версию HTTP и принимаемые браузером языки.
2. Укажите IP-адреса вашего компьютера и сервера.
3. Есть ли в первом запросе HTTP GET строка «IF-MODIFIED-SINCE»?
4. Проанализируйте ответ сервера на первый запрос: передал ли серверявным образом содержимое запрашиваемого ресурса?
5. Теперь просмотрите содержимое второго запроса HTTP GET: есть литам строка

«IF-MODIFIED-SINCE» (какую информацию содержит)?

6. Что означает код состояния в ответе сервера на второй запрос HTTP GET? Передал ли сервер явным образом содержимое запрашиваемогоресурса?

Вариант 3. DNS

1) очистить кэш DNS с помощью *ipconfig* (в командной строке)*:*

ipconfig /flushdns

2) очистить кэш браузера;

3) запустить *Wireshark;*

4) настроить фильтр: ip.addr == ваш_IP_адрес;

5) запустить процесс захвата трафика;

6) URL: например, http://www.ietf.org/;

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

7) остановить захват трафика.

Ответьте на следующие вопросы.

1. Найдите DNS-запрос и ответ. Поверх какого протокола транспортного уровня работает DNS?
2. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
3. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес садресом вашего DNS-сервера?
4. Укажите тип DNS-запроса.
5. Что содержится в поле «Answers» DNS-ответа?
6. Проверьте, какой IP-адрес содержится в последующем пакете TCPSYN, который был отправлен вашим компьютером.
7. Формирует ли ваш компьютер новые DNS-запросы для получения содержащихся на сайте изображений?

Вариант 4. DNS

nslookup — утилита, предоставляющая пользователю интерфейс командойстроки для обращения к системе DNS (проще говоря, DNS-клиент).

Позволяет задавать различные типы запросов и запрашивать произвольноуказываемые сервера.

Использование *nslookup:*

nslookup [-opt ...]

интерактивный режим с использованием сервера по умолчанию nslookup [-opt ...] - server

интерактивный режим с использованием сервера "server" nslookup [-opt ...] host

поиск узла "host" с использованием сервера по умолчанию nslookup [-opt ...] host server

поиск узла "host" с использованием сервера "server"

1) запустить *Wireshark;*

2) настроить фильтр: ip.addr == ваш_IP_адрес;

3) запустить процесс захвата трафика;

4) в командной строке:

nslookup host

например, nslookup sspu.ru

в качестве узла (host) использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Прим.: Всего *nslookup* отправил три DNS-запроса и получил три DNS- ответа. Для дальнейшего анализа использовать последние два пакета. (Первые два набора запросов/ответов не генерируются стандартными интернет-приложениями и специфичны для *nslookup*.)

Ответьте на следующие вопросы.

1. Найдите DNS-запрос и ответ. Поверх какого протокола транспортного уровня работает DNS?
2. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
3. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес садресом вашего DNS-сервера?
4. Укажите тип DNS-запроса.
5. Что содержится в поле «Answers» DNS-ответа?

Повторите предыдущий эксперимент, но в командной строке введитекоманду:

nslookup -type=NS host

например, nslookup -type=NS ifmo.ru

в качестве узла (host) использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

Ответьте на следующие вопросы.

1. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
2. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес садресом вашего DNS-сервера?

3. Укажите тип DNS-запроса.
4. Проанализируйте DNS-ответ: укажите имена серверов, возвращающих авторитативный отклик.

Вариант 5. ICMP

1) запустить *Wireshark;*

2) настроить фильтр (icmp);

3) запустить процесс захвата трафика;

4) в командной строке:

ping –n 10 конечный_узел например, ping –n 10 wireshark.org

в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Ответьте на следующие вопросы.

1. Сколько всего пакетов захватила программа? Почему?
2. Какой IP-адрес вашего компьютера, адрес назначения?
3. Проанализируйте ping request, отправленный с вашего компьютера: укажите тип и код ICMP. Какие еще поля содержит ICMP пакет? Сколько байт занимают поля «Checksum», «Sequence number», «Identifier»?
4. Проанализируйте ping reply: укажите тип и код ICMP. Какие еще поля содержит ICMP пакет? Сколько байт занимают поля «Checksum», «Sequence number», «Identifier»?

6) запустить *Wireshark;*

7) настроить фильтр (icmp);

8) запустить процесс захвата трафика;

9) в командной строке: tracert

конечный_узел

например, tracert wireshark.org

в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

10) остановить захват трафика.

Ответьте на следующие вопросы.

1. Какой IP-адрес вашего компьютера, адрес назначения?

2. Проанализируйте пакет ICMP echo: отличаются ли эти пакеты отпакетов в первой части эксперимента? Чем?
3. Проанализируйте пакет ICMP error: какие поля в нем содержатся?
4. Чем отличаются пакеты ICMP reply (полученные) и ICMP error?

Вариант 6. DHCP

1) в командной строке:

ipconfig /release (IP-адрес станет 0.0.0.0)

2) запустить *Wireshark;*

3) настроить фильтр (bootp);

4) запустить процесс захвата трафика;

5) в командной строке:

ipconfig /renew (получение нового IP-адреса)и еще раз:

ipconfig /releaseipconfig /renew

6) остановить захват трафика.

Ответьте на следующие вопросы.

1. Поверх какого протокола транспортного уровня работает DHCP?
2. Нарисуйте временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номерапортов источника, назначения.
3. Какими значениями отличаются пакеты DHCP Discover и DHCPRequest?
4. Укажите значения поля «Transaction-ID» для всех пакетов (Discover/Offer/Request/ACK), что это поле означает?
5. Укажите IP-адреса источника, назначения для всех пакетов.
6. Укажите IP-адрес DHCP сервера.
7. Поясните назначение сообщения DHCP release.
8. Очистите фильтр. Появились ли пакеты ARP, отправленные илиполученные в течение обмена DHCP пакетами? Почему?

Вариант 7. Ethernet и ARPEthernet

1) очистить кэш браузера;

2) запустить *Wireshark;*

3) запустить процесс захвата трафика;

4) URL: например, http://ru.wikipedia.org/wiki/Ethernet

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика;

6) в меню «Analyze» → «Enabled Protocols» можно снять галочку IP:тогда вписке пакетов не будет отображаться информация по протоколам верхнего уровня (после IP) — необязательный пункт.

Выберите кадр Ethernet, содержащий сообщение HTTP GET.Ответьте на следующие вопросы.

1. Укажите 48-битный Ethernet адрес вашего компьютера.
2. Укажите 48-битный Ethernet адрес назначения. Что это за адрес?(Адрес сервера?)
3. Укажите 16-чное значение двухбайтового поля «Type»: какомупротоколу верхнего уровня оно соответствует?

Выберите кадр Ethernet, содержащий ответ HTTP. Ответьте на следующие вопросы.

1. Укажите значение Ethernet адреса источника. Какое устройствоимеет такой адрес?
2. Укажите Ethernet адрес назначения: это адрес вашего компьютера?
3. Укажите 16-чное значение двухбайтового поля «Type»: какомупротоколу верхнего уровня оно соответствует?

ARP

1) очистить ARP кэш:

«Пуск» → «Выполнить»: netsh interface ip delete arpcache

Вывести на экран ARP-таблицу можно с помощью команды: arp –a

2) очистить кэш браузера;

3) запустить *Wireshark;*

4) запустить процесс захвата трафика;

5) URL: например, http://ru.wikipedia.org/wiki/Ethernet

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

6) остановить захват трафика;

7) в меню «Analyze» → «Enabled Protocols» снять галочку IP: в списке пакетов теперь не будет отображаться информация по протоколамверхнего уровня (после IP) — необязательный пункт.

Ответьте на следующие вопросы.

1. Укажите 16-чные значения адресов источника и назначения впакете, содержащем ARP запрос (ARP ответ).
2. Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует (для ARP запроса/ARPответа)?
3. Укажите значение поля «opcode» (для ARP запроса/ARP ответа).
4. Содержит ли ARP запрос IP-адрес источника (для ARP запроса/ARPответа)?

Вариант 8. FTP

1) запустить *Wireshark;*

2) запустить процесс захвата трафика;

3) скачать файл с FTP-сервера (например, ftp://ftp.canon.ru/);

в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

4) остановить захват трафика;

5) настроить фильтр (ftp || ftp-data).Ответьте

на следующие вопросы.

1. Сколько байт данных содержится в пакете FTP-DATA?
2. Укажите IP-адреса FTP-сервера и вашего компьютера.
3. Укажите MAC-адрес FTP-сервера.
4. Укажите протокол транспортного уровня, который используетпротокол FTP.
5. Укажите порт, который используется при передаче данных попротоколу FTP.
6. Поясните, чем отличаются пакеты FTP и FTP-DATA.

Вариант 9. UDP

1) запустить *Wireshark;*

2) настроить фильтр (udp);

3) запустить процесс захвата трафика;

4) создать сеанс связи с помощью программы *TeamViewer*;

5) остановить захват трафика.

Прим.: можно ничего не делать, просто запустить захват трафика — UDP пакеты все равно найдутся.

Ответьте на следующие вопросы.

1. Выберите один UDP пакет из списка пакетов. Сколько полей в UDPзаголовке?

Что это за поля?
2. Какова длина (в байтах) каждого поля заголовка?
3. Длина чего указана в поле «Length»?
4. Какова максимальная длина поля данных UDP?
5. Какой максимально возможный номер порта источника?
6. Укажите номер протокола для UDP (см. соответствующее поле IP-дейтаграммы) в 10-чном и 16-чном виде.
7. Найдите пару пакетов: первый UDP пакет, отправленный вашим компьютером, и ответ на него.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если все шаги выполнены полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 4. Отчёт об аудите безопасности АИС

Тематика: Классификация уязвимостей АИС.

Текст задания: Ознакомьтесь со списком уязвимостей, представленных на сайте ФСТЭК России: https://bdu.fstec.ru/vul

Найдите и приведите описание (код в классификациях BDU и CVE, описание на сайте ФСТЭК, версия программного обеспечения, в котором обнаружена уязвимость, нарушаемые свойства безопасности информационных ресурсов, к которым приводит эксплуатация уязвимости):

- Не менее двух уязвимостей, выявленных в какой-либо версии браузера Google Chrome (Производитель: Google Inc.);
- Не менее двух уязвимостей, выявленных в какой-либо версии операционной системы Windows (Производитель: Microsoft Corp.);

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если представлено полное описание уязвимостей в соответствии с текстом задания;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности при описании уязвимостей;

Оценка «удовлетворительно» выставляется, когда аспирантом была найдена уязвимость только для одного и программных продуктов.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 5. Методическое обеспечение аудита информационной безопасности

Тематика: Основные классификационные признаки компьютерных вирусов. Технологии обнаружения заражения вирусами.

Текст задания:

Ознакомьтесь с описанием компьютерных вирусов на официальном сайте антивируса Dr. Web: https://vms.drweb.ru/virustypes/

Определите, к какому типу относятся следующие вирусы:

- W97M.DownLoader.507: https://vms.drweb.ru/virus/?i=7325800
- PowerShell.DownLoader.72: https://vms.drweb.ru/virus/?i=15265315
- Win32.HLLW.Autoruner: https://vms.drweb.ru/virus/?i=115441

Являются ли вирусами Adware.Cootek.1.origin (https://vms.drweb.ru/virus/?i=14973923) и Adware.SaveNow (https://vms.drweb.ru/virus/?i=8914)?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» выставляется, если аспирант ошибся при ответе на один вопрос;

Оценка «удовлетворительно» выставляется, если аспирант ошибся при ответе на два вопроса.

Оценка «неудовлетворительно» выставляется, если аспирант допустил больше двух ошибок.

Практическое занятие 6. Корпоративная политика информационной безопасности

Тематика: Корпоративная политика безопасности; организационно-распорядительные документы организации.

Текст задания: В компьютерном классе установлена программа Deep Freeze. Это позволяет системному администратору отказаться от установки антивирусного программного обеспечения, но вынуждает составить инструкцию по работе за компьютерами для педагогов, проводящих занятия в этом кабинете. Что, по вашему мнению, следует включить в эту инструкцию?

Какие ещё отрицательные стороны вносят в образовательный процесс подобные программы? Какова их положительная роль для образовательного учреждения?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ, но при ответе допущены недочеты, изложение недостаточно систематизированное, в выводах и обобщениях имеются некоторые неточности;

Оценка «удовлетворительно» выставляется, если аспирант обнаруживает поверхностные знания, допускает ошибки при ответе на любой из представленных во втором абзаце вопросов (или не дает на него ответа).

Оценка «неудовлетворительно» выставляется, если аспирант допускает ошибки при ответе на вопрос из первого абзаца.

Практическое занятие 7. Инструментальные средства аудита ИБ

Тематика: Методы и инструментальные средства проведения активного аудита ИБ.

Постановка задачи:

Это задание повышенной сложности. Его выполнение необходимо, чтобы получить оценку «отлично».

В соответствии с заданием варианта А или Б требуется сгенерировать и отправить в сеть трафик с заданными параметрами. Убедиться в том, что передача пакетов действительно происходит, можно с помощью *Wireshark.*

В отчете нужно привести структуру генерируемого пакета и параметры генерации (можно в виде скриншотов Wireshark или Ostinato). Во время защиты необходимо предоставить по требованию преподавателя pcap-файл с дампом сгенерированного трафика.

Описание программы Ostinato:

Прим.: для работы с генератором *Ostinato* нужны права администратора.

1. Рабочая область (рис. 3) поделена на 3 части: список портов (*portslist*), список потоков (*streams list*), окно статистики (*statistics window*).
2. В списке портов вы увидите группу портов для «127.0.0.1» состатусом «присоединена» (*connected*) (зеленый цвет).
3. Выберите порт из группы портов.
4. В списке потоков создайте новый поток: правой кнопкой → *Newstream.*
5. Для редактирования созданного потока дважды щелкните наиконке потока (или правой кнопкой → *Edit stream*).
6. В окне редактирования потока выберите протоколы, заполнитеполя, определите количество пакетов, скорость. Нажмите «OK».
7. **Важно!** Нажмите кнопку *Apply,* которая расположена сверхусписка потоков.

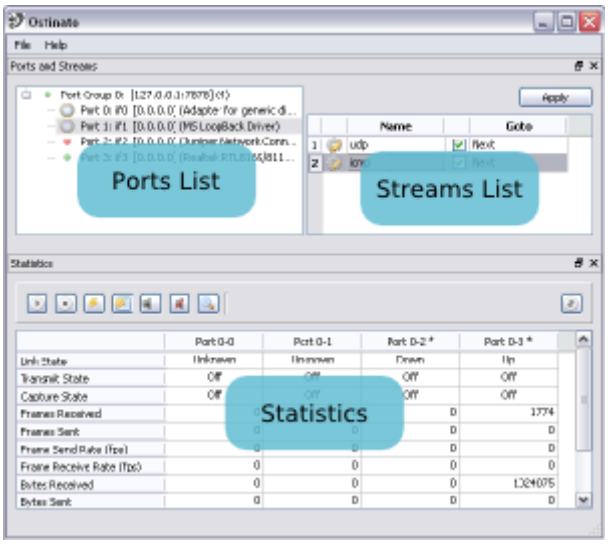


Рис. 3. Главное окно программы *Ostinato*

8. **Важно!** В окне статистики выберите тот же порт, для которого высоздавали поток (выделите весь столбец, щелкнув на заголовке порта).
9. Нажмите кнопку *Start Transmit.*

Клиент-серверная архитектура

Генератор имеет клиент-серверную архитектуру. Запущенный на одном компьютере клиент (*ostinato*) соединен с одним (или несколькими) компьютером-сервером (*drone*). Клиент имеет доступ ко всем портам всех присоединенных серверов и осуществляет управление ими. В один момент времени сервер может быть соединен только с одним клиентом. Клиент и сервер могут быть запущены на разных ОС (например, клиент Windows может быть соединен как с сервером Windows, так и Linux). Режим по умолчанию — клиент и сервер запущены на одном компьютере. Локальный сервер представлен loopback IP-адресом 127.0.0.1.

Важно! Клиент отправляет серверу конфигурационную информацию по потоку, только если была нажата кнопка *Apply*. Поэтому если вы добавляете/редактируете/удаляете потоки, не забывайте нажимать *Apply*,иначе изменения не будут сохранены.

Список портов (Ports List)

Список портов (рис. 4) отображает все порты, которые можно контролировать. Порты объединены в следующие группы портов. Группа портов это компьютер или устройство (локальное или удаленное), запущенное на серверном компоненте (*drone*). Ниже перечислены статусы группы портов:

	Клиент не соединен с группой портов
	Клиент пытается соединиться с группой портов
	Клиент соединен с группой портов
	Клиентом обнаружена ошибка при попытке соединения с группойпортов

Статусы портов. Порты могут иметь следующие статусы:

	Текущий статус порта неизвестен
	Порт не присоединен
	Порт присоединен

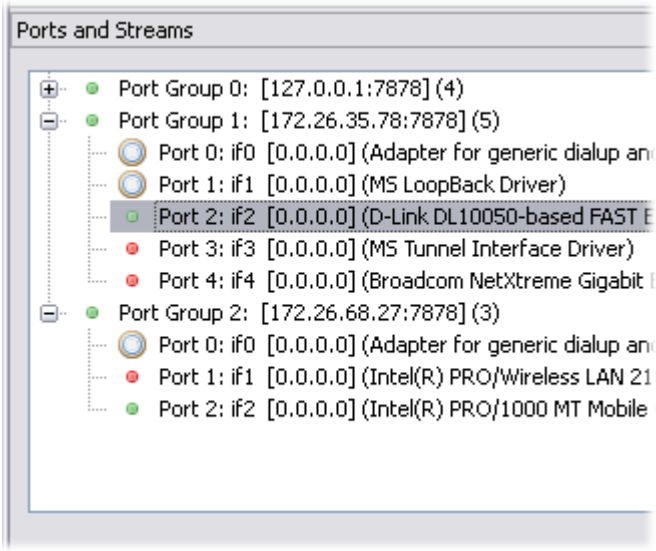


Рис. 4. Список портов

Прим.: Если доступ к порту запрещен администратором, порт может не отображаться. Если в списке нет ни одного порта, проверьте, запущен ли серверный компонент (*drone*) с правами администратора.

Действия над группами портов

Значок	Действие	Описание
	New Port Group	Добавить новый удаленный компьютер к спискуи произвести соединение. Нужно указать IP- адрес и дополнительно (необязательно) номер порта.
	Delete Port Group	Удалить удаленный компьютер из списка
	Connect Port Group	Произвести попытку переподключения к удаленному компьютеру
	Disconnect Port Group	Отсоединить удаленный компьютер (он не будетудален из списка, при необходимости можно присоединить его снова)
	Exclusive Port Control	Для предотвращения использования порта операционной системой можно установить полный контроль над портом
	Port Configuration	Конфигурирование свойств порта

Контроль нескольких компьютеров

1. На удаленном компьютере, за которым вы хотите осуществлятьконтроль, запустите серверный компонент (*drone*).
2. В клиенте *Ostinato* выберите *File → New Port Group* и введите IP-адрес.
3. Удаленный компьютер появится как новая группа портов в спискепортов.

Вы можете присоединить любое количество удаленных компьютеров.

Конфигурирование портов

Режим передачи (Transmit Mode)

Sequential Streams: потоки отправляются один за другим последовательно. Все пакеты одного потока будут отправлены после окончания передачи пакетов предшествующего потока.

Пример. Есть 2 потока: TCP и UDP. TCP поток сконфигурированследующим образом: 100 пакетов, скорость передачи 10 пакетов/с. UDP поток сконфигурирован следующим образом: 500 пакетов, скорость передачи 5 пакетов/с. В данном режиме сначала будут отправлены 100 пакетов TCP со скоростью 10 пакетов/с, а затем — 500 пакетов UDP со скоростью 5 пакетов/с.

Interleaved Streams: потоки отправляются в зависимости от их скорости (packet/burst rate). Пакеты всех потоков будут отправлены в чередующемся режиме. Это непрерывный режим — вы можете указать скорость передачи (packet/burst rate), но не количество пакетов.

Пример. Есть 2 потока: TCP и UDP. TCP поток сконфигурированследующим образом: скорость передачи 10 пакетов/с. UDP поток сконфигурирован следующим образом: скорость передачи 5 пакетов/с. В данном режиме за секунду будут отправлены 15 пакетов, из которых 10 пакетов — пакеты TCP, а 5 — UDP.

Создание, редактирование и удаление потоков

Чтобы создать поток, сначала выберите соответствующий порт в списке портов, далее — *File → New Stream* (или правой кнопкой в контекстном меню).

Для того чтобы вставить поток между двумя существующими потоками, выберите нижний поток и затем создайте новый (он будет создан перед выделенным). Дважды щелкните на ячейке *Name* и присвойте потоку нужное имя. Поток можно запретить/разрешить, сняв/поставив галочку. Столбец *Goto* позволяет задать способ передачи потоков: по умолчанию *Next* — после завершения передачи потока генератор *Ostinato* переходит к отправке следующего по списку.

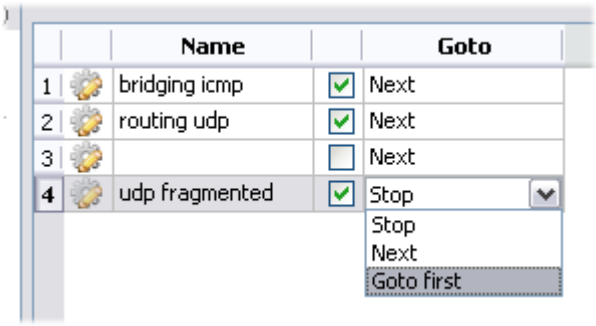


Рис. 5. Список потоков

Для удаления потока выберите поток, затем *File → Delete Stream* (илиправой кнопкой в контекстном меню).

Открытие, сохранение потоков

Чтобы открыть файл, содержащий пакеты, выберите соответствующий порт в списке портов, затем *File → Open Streams* (или правой кнопкой в контекстном меню). Чтобы сохранить сконфигурированные пакеты, выберите соответствующий порт в списке портов, затем *File → Save Streams* (или правой кнопкой в контекстном меню). Форматы файлов: PCAP, PDML, собственный формат.

Конфигурирование потоков

Выберите *File → Edit Stream:*

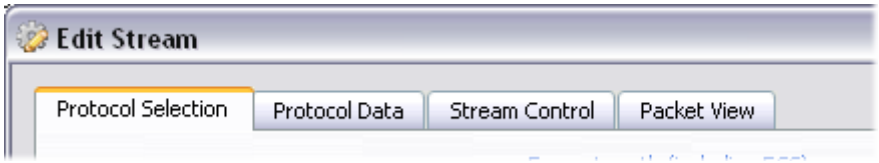


Рис. 6. Окно редактирования потока

Выбор протокола
Длина кадра

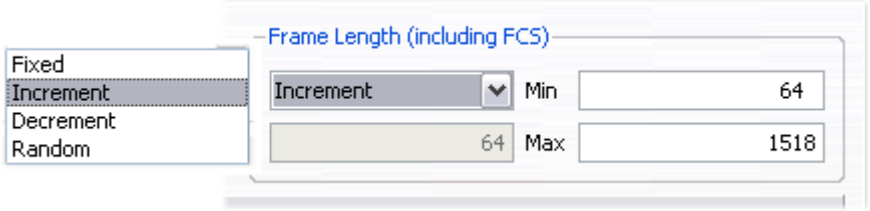


Рис. 7. Фрагмент окна редактирования потока: выбор длины кадра Вы можете установить фиксированное значение *(fixed)* длины кадра или одно из трех других:

инкрементированное *(incrementing)*, декрементированное *(decrementing)*, случайное *(random)*.

Прим.: для нефиксированных значений следует конфигурировать поток из нескольких пакетов, иначе разница в длине кадра не будет заметна.

Прим.: значение длины кадра включает в себя 4 байта FCS.

Протоколы (простой режим)

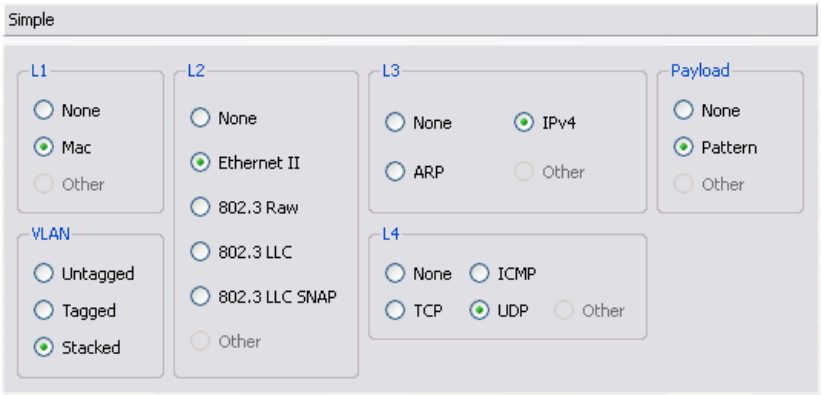


Рис. 8. Фрагмент окна редактирования потока: выбор протокола (простойрежим)

Выбор из стандартных комбинаций различных протоколов осуществляется с помощью переключателей.

Для нестандартных комбинаций следует выбрать расширенный режим *(advanced mode)*.

Протоколы (расширенный режим)

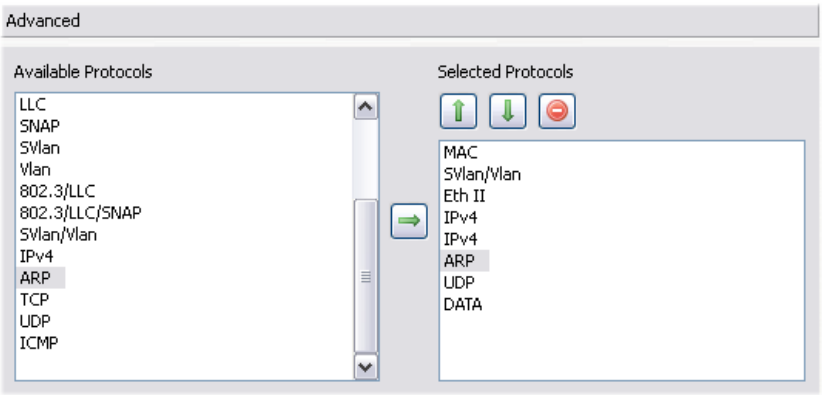


Рис. 9. Фрагмент окна редактирования потока: выбор протокола (расширенный режим)

В данном режиме протоколы можно «собирать» в любом порядке (например, TCP после ARP; IP над IP).

Слева на рис. 9 отображены все доступные протоколы, справа — выбранные из списка доступных.

	Добавить выбранный(ые) протокол(ы) из левого списка в правый
	Переместить выбранный протокол вниз
	Переместить выбранный протокол вверх
	Удалить выбранный протокол из правого списка

Поля протокола

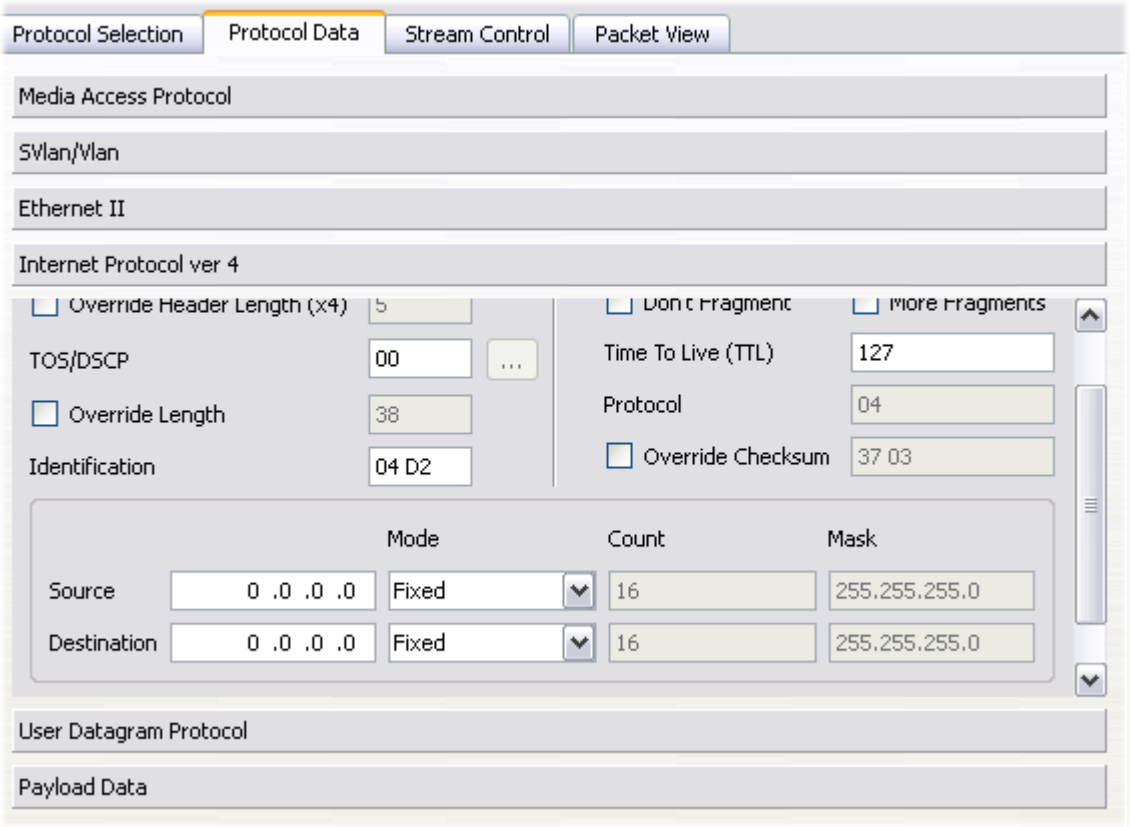


Рис. 10. Фрагмент окна редактирования потока: вкладка «Protocol Data»

Конфигурируйте поля каждого протокола.

Прим.: поля *Protocol Id* для поддерживаемых протоколов не редактируются (например, если после Ethernet идет IP, будет установлено значение 0x0800 без возможности его изменения).

Управление потоками

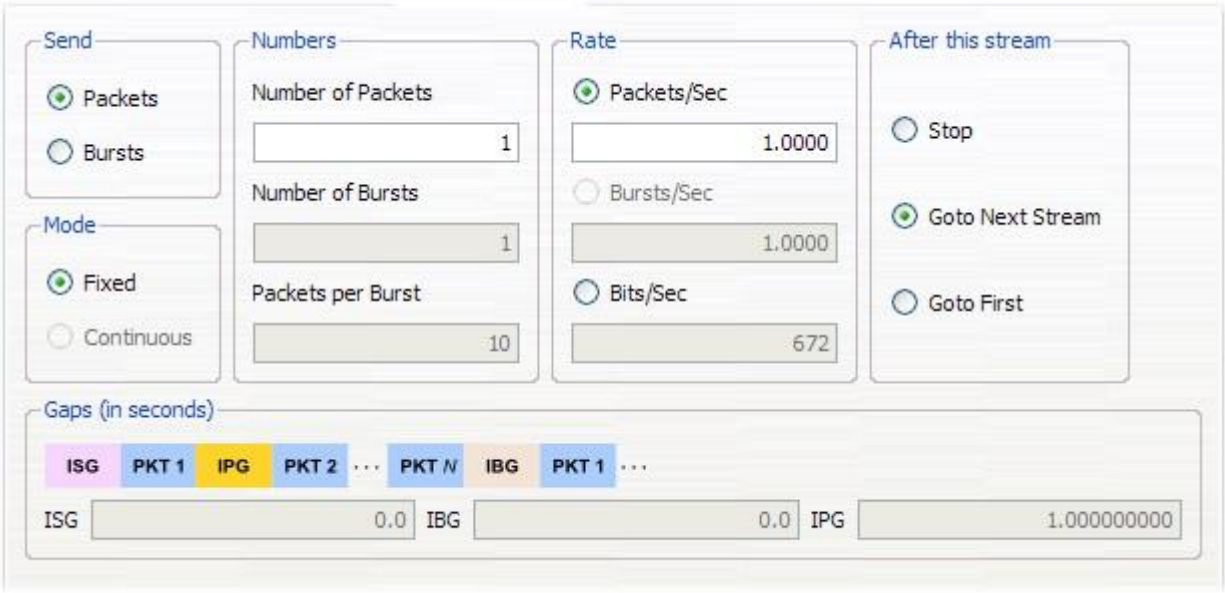


Рис. 11. Фрагмент окна редактирования потока: вкладка «Stream Control»

Варианты отправки:

1) отправлять пакеты (packets) — можно задавать их количество и скорость отправки (pkts/sec);
2) отправлять группы пакетов (bursts) — можно задавать их количество и скорость отправки (bursts/sec), дополнительно: количество пакетовв группе.

Также можно задать порядок передачи: *goto the next stream* (перейти кследующему в списке потоку), *goto first* (перейти к первому потоку в списке), *stop* (остановить передачу).

Прим.: в зависимости от режима отправки некоторые поля могут бытьнедоступны.

Важно! Генератор *Ostinato* не гарантирует отправку пакетов с заданной скоростью. Фактическая скорость зависит от компьютера (например, от его загрузки), на котором запущен серверный компонент(*drone*).

Просмотр пакета

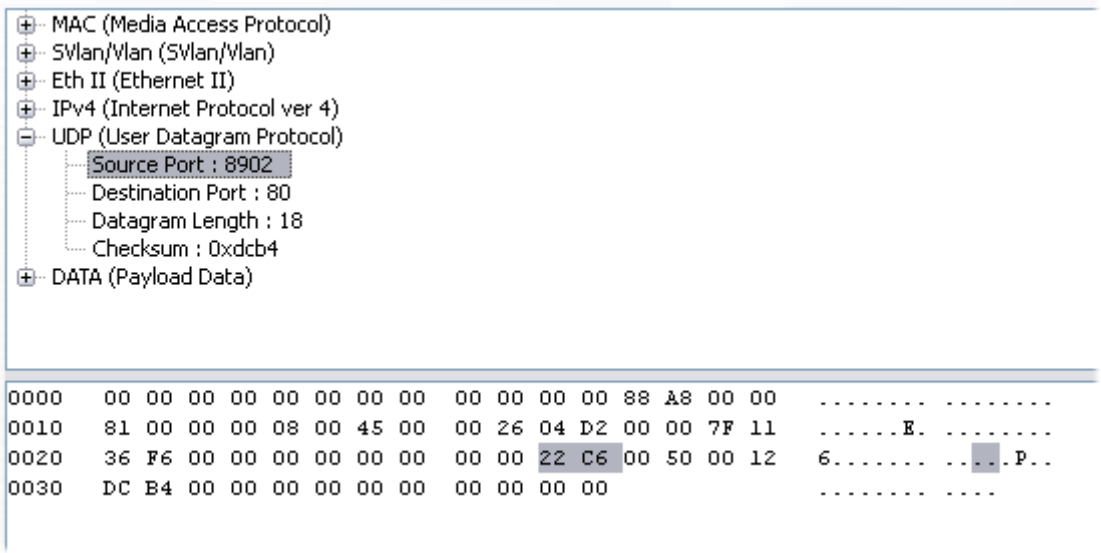


Рис. 12. Фрагмент окна редактирования потока: вкладка «Packet View»

Здесь полностью представлен сконфигурированный пакет: в видедерева и в 16-чной форме.

Окно статистики

Все кнопки, расположенные в этом окне (кроме *Clear All Stats*), применимы к выбранному(ым) порту(ам) в самом окне (не в списке портов).

Порт выбран, если выделен весь столбец целиком, а не его часть.

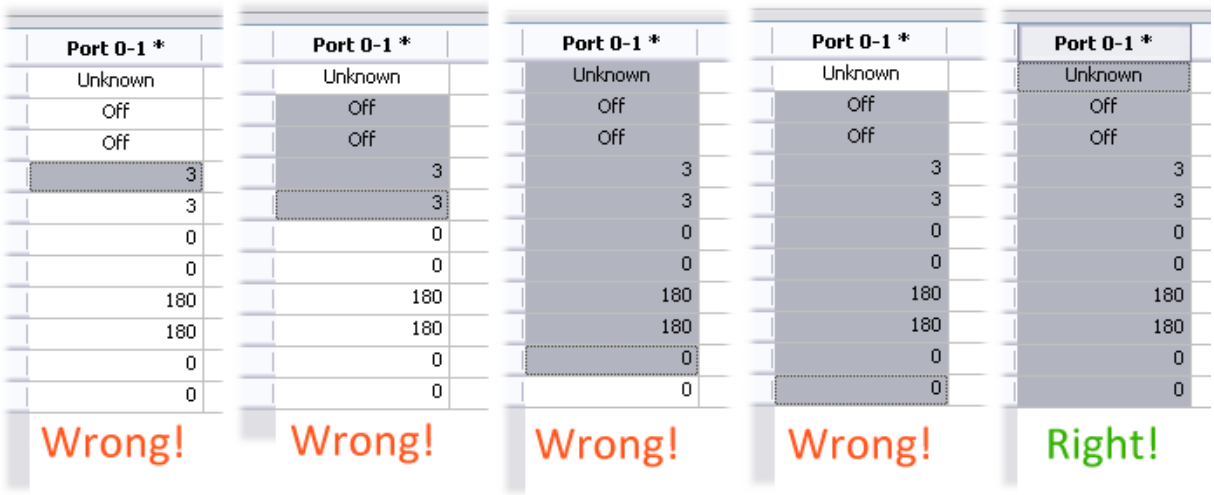


Рис. 13. Окно статистики

Действия

Значок	Действие	Описание
	Start Transmit	Начать передачу пакетов на выбранный(ые)порт(ы)
	Stop Transmit	Остановить передачу пакетов на выбранный(ые)порт(ы)
	Clear Stats	Очистить статистику выбранного(ых) порта(ов)
	Clear All Stats	Очистить статистику всех портов
	Start Capture	Начать захват пакетов с выбранного(ых) порта(ов)
	Stop Capture	Остановить захват пакетов с выбранного(ых) порта(ов)
	ConfigureView	Выбрать очередность отображения порта(ов) вокне статистики

Вариант А

Генерировать два потока пакетов в соответствии с таблицей 1. Цифра обозначает номер варианта. Например, для 1-го варианта: один поток ARP, второй Ethernet, т.к. цифра «1» находится на пересечениистроки ARP и столбца Ethernet.

Таблица 1

	ARP	Ethernet	ICMP	IP	TCP	UDP
ARP		1	2	3	4	5
Ethernet			6	7	8	9
ICMP				10	11	12
IP					13	14
TCP						15
UDP						

Использовать два режима передачи:

1) *Sequential Streams* (см. в описании программы *Ostinato*);

2) *Interleaved Streams* (см. в описании программы *Ostinato*).

Таблица 2

Параметры						
Размер пакетов	Скорость передачи	Адреса отправителя, назначения	Порт источника, назначения	MAC-адрес	Фрагмен-тация	Количество пакетов
Любой	Любая	Фиксированные	В соответствии с протоколом	Фиксированный	Рассмотреть два варианта: без фрагментации и с фрагментацией	> 2

Вариант Б

Генерировать тот же тип пакетов, что и в первой части работы. Можно генерировать несколько потоков пакетов.

Использовать два режима передачи:

1) *Sequential Streams* (см. в описании программы *Ostinato*);
2) *Interleaved Streams* (см. в описании программы *Ostinato*).

Таблица 2

Параметры						
Размер пакетов	Скорость передачи	Адреса отправителя, назначения	Порт источника, назначения	MAC-адрес	Фрагментация	Количество пакетов
Любой	Любая	Фиксированные	В соответствии с протоколом	Фиксированный	Рассмотреть два варианта: без фрагментации и с фрагментацией	> 2

В отчете привести структуру генерируемого пакета и параметры генерации. Убедиться в том, что передача пакетов действительно происходит, можно с помощью *Wireshark.*

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если все шаги выполнены полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 8. Изучение практического опыта технического аудита безопасности АИС предприятий

Тематика: Анализ опыта и рекомендации по планированию: отчетные материалы.

Текст задания:

Проанализировать содержание файлов, расположенных по ссылке (https://disk.yandex.ru/d/A-yhewASIvcSRw):

- Разработка и внедрение опытного образца КСИБ (doc, раздел «Техническое задание»);
- Техническое задание на оказание услуг по проведению аудита информационной безопасности (doc);
- Техническое задание по созданию системы защиты (docx).

Представить основные разделы, содержащиеся в данных документах, в виде схемы (или ментальной карты) с краткими пояснениями.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если работа выполнена полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 9. Заключительное занятие. Подведение и анализ промежуточных результатов освоения дисциплины

При подготовке материалов для заключительного практического занятия, преподаватель учитывает недостаточную степень развития навыков аспирантов, определенную в ходе практических занятий и при оценке самостоятельной работы. На практическом занятии обсуждаются итоги проведения занятий по дисциплине, проверяется полнота и качество собранного аспирантом портфолио материалов и результатов выполнения заданий по дисциплине. Обсуждаются вопросы, вынесенные для проведения зачета с оценкой, итоги выполнения работы по написанию рефератов. Оцениваются индивидуальные достижения, полученные аспирантов в ходе внеурочной работы (сертификаты олимпиад, конкурсов, грантов, написание тезисов/статей в сборники конференций различного уровня).

3. Методические указания по выполнению других видов самостоятельной работы по дисциплине

ТЕМЫ РЕФЕРАТОВ

1. Проблемы защиты информации в открытых информационных системах
2. Модели защиты информации открытых ИС
3. Особенности защиты информации в открытых ИС
4. Требования к архитектуре информационных систем для обеспечения безопасности их функционирования
5. Уровни защищённости информационных систем
6. Аудит выделенных помещений
7. Информационная безопасность в научной и образовательной средах
8. Организация аудита информационной безопасности в кредитной организации
9. Инженерно-техническая защита объектов инфокоммуникаций

Критерии оценки

Оценки в баллах	Критерии
2	Самостоятельность в подготовке материала
3	Аргументированность и полнота материала
2	Использование современной и актуальной литературы
3	Качество презентации
10	**Итого**

Шкала оценивания:

– оценка «отлично» выставляется аспиранту, если сумма баллов по всем критериям равна 9-10 баллам;

– оценка «хорошо» выставляется аспиранту, если сумма баллов по всем критериям равна 7-8 баллам;

– оценка «удовлетворительно» выставляется аспиранту, если сумма баллов по всем критериям равна 5-6 баллам;

– оценка «неудовлетворительно» выставляется аспиранту, если сумма баллов по всем критериям равна 1-4 баллам.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ЗАЧЕТА С ОЦЕНКОЙ

1. Понятие многоуровневой защиты. Основные механизмы обеспечения сетевой безопасности
2. Модель многоуровневой защищенной корпоративной сети. Защита от атак в ЛВС
3. Основные элементы архитектуры межсетевых экранов
4. Основные нормативные документы, используемые при организации аудита
5. Сущность аудита информационной безопасности
6. Особенности автоматизированных информационных систем как объектов аудита ИБ
7. Основные характеристики информационного и организационно-методического обеспечения безопасности функционирования организаций

8. Положение о внутреннем аудите организации.
9. Цели и виды аудита информационной безопасности
10. Этапы проведения аудита
11. Принципы и формы аудита ИБ
12. Основные и дополнительные задачи внутреннего аудита безопасности информационных систем
13. Этапы и содержание работ по проведению аудита ИБ
14. Технология сбора информации аудита
15. Планирование и осуществление процедуры аудита
16. Методика подготовки аудитора
17. Основные подходы к анализу данных
18. Задачи анализа и управления рисками информационной безопасности
19. Обязанности и правила этики аудитора
20. Анализ организационно-распорядительной документации по обеспечению режима информационной безопасности
21. Обоснование требований по результатам оценки рисков.
22. Методика подготовки отчётных документов после проведенного аудита, структура и содержание отчёта
23. Рекомендации организации, предприятию по результатам аудита
24. Классификация уязвимостей АИС.
25. Методы и подходы к управлению рисками информационной безопасности
26. Основные классификационные признаки компьютерных вирусов
27. Технологии обнаружения заражения вирусами
28. Документация системы управления информационной безопасностью
29. Концепция и корпоративная политика ИБ, методы их формирования
30. Определение требуемого уровня ИБ
31. Ядро системы комплексной защиты информации
32. Ресурсы комплексной системы защиты информации
33. Методы сбора исходных данных
34. Методы и инструментальные средства проведения активного аудита ИБ
35. Возможности сканеров безопасности, мониторинг событий безопасности

По представленным вопросам предполагается выполнение аспирантом конспектов или повторение материала с использованием конспектов лекций.

4. Примеры контрольных заданий (оценочных средств), используемых при текущем контроле успеваемости и промежуточной аттестации по дисциплине

Демоверсия итогового тестирования:

1. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

а) выработка и проведение в жизнь единой политики безопасности (правильный ответ);

б) унификация аппаратно-программных платформ;

в) минимизация числа используемых приложений;

г) использование собственных линий связи;

д) обеспечение конфиденциальности и целостности при сетевых взаимодействиях (правильный ответ);

е) полный анализ сетевого трафика;

2. Экранирование на сетевом и транспортном уровнях может обеспечить:

а) разграничение доступа по сетевым адресам (правильный ответ);

б) выборочное выполнение команд прикладного протокола;

в) контроль объема данных, переданных по TCP-соединению (правильный ответ);

3. Укажите федеральные органы исполнительной власти, уполномоченные в области безопасности информации:

а) Служба внешней разведки РФ;

б) Федеральная служба по техническому и экспортному контролю РФ (правильный ответ);

в) Федеральная служба охраны РФ;

г) Федеральная служба безопасности РФ (правильный ответ);

4. К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации?

а) законодательный;

б) административный (правильный ответ);

в) процедурный;

г) научно-технический;

5. Определите процедуру, которая должна быть проведена с целью оценки соответствия требованиям по безопасности информации принятых на объекте мер по защите информации:

а) Сертификация;

б) Аттестация (правильный ответ);

в) Аккредитация;

г) Лицензирование;

6. Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты от несанкционированных изменений программной и аппаратной среды ПЭВМ?

а) Регистрации и учета;

б) Криптографической защиты;

в) Обеспечения целостности (правильный ответ);

г) Управления доступом.

7. При каком принципе управления доступом уполномоченный пользователь получает доступ к документам заданного уровня конфиденциальности?

а) Дискреционный;

б) Мандатный (правильный ответ);

8. К какому виду мер относится мера: использование специальных звукоизолирующих экранов на элементах систем отопления и вентиляции?

а) Организационная;

б) Техническая (правильный ответ).

Автор(ы)-составитель(и): *Привалов А.Н.*, профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор