дисциплина
АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛЕКЦИЯ

ОСНОВНЫЕ ПОЛОЖЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Москва - 2013

ВОПРОСЫ

1. Основные направления деятельности в области аудита безопасности информации

2.Виды аудита информационной безопасности

3. Аудит выделенных помещений

ЛИТЕРАТУРА

site http://www.ipcpscience.ru/ → **ОБУЧЕНИЕ**

- *Мельников В. П.* Информационная безопасность : учеб. пособие / В.П.Мельников, С.А.Клейменов, А.М.Петраков ; под ред. С.А.Клейменова. — М.: Изд. центр «Академия», 2005.
- *Партыка Т.Л.* Информационная безопасность : учеб. пособие / Т.Л.Партыка, И.И.Попов. — М. : Форум : Инфра-М, 2002.
- *Юзвишин И. И.* Основы информациологии : учебник / И. И. Юзви-шин. — 3-е изд., перераб. и доп. — М.: Высш. шк., 2001
- *Абдикеев Н. М.* Автоматизированные информационные систе-мы в производстве, маркетинге и финансах: учеб. пособие / Под общ. ред. К. И. Курбакова. М.: КОС ИНФ, Рос. экон. акад., 2003.
- *Емельянова Н. З., Партыка Т. Л., Попов И. И.* Основы построения автоматизированных информационных систем: учебное пособие. М.: ФОРУМ: ИНФРА-М, 2005.
- **Стандарт ISO-IEC 17799:2005**
- **ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью**
- **ISO/IEC 27002:2005** Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью (ранее ISO/IEC 17799:2005).
- **Information technology. Guidelines for the management of IT security. Management guidance of network security** (Информационные технологии. Руководство по управлению ИТ безопасностью. Руководство по управлению сетевой безопасностью)
- **Information technology. Guidelines for the management of IT security. Selection of safeguards** (Информационные технологии. Руководство по управлению ИТ безопасностью. Выбор механизмов защиты)

Вопрос 1

Основные направления деятельности в области аудита безопасности информации

Девиз аудита информационной безопасности
- доверяй, но проверяй

Постулаты аудита ИБ

- Угрозы легче предупредить, чем устранять результаты их воздействия.
- На бога надейся, а сам не плошай.
- Дружба дружбой, а табачок врозь.

Федеральный нормативный акт	Определение понятия информация
Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»	информация - сведения (сообщения, данные) независимо от формы их представления
Федеральный закон от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации» (не действует)	информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»	информация, составляющая коммерческую тайну, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны
Закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне»	государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

ОСНОВНЫЕ ПОНЯТИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

audit ['O:dIt] n – проверка, ревизия

«Аудит информационных систем — это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании» («Консалтинг и аудит в сфере ИТ 2004». CNews Analytics).

Аудит информационной безопасности – специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам.

«Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности» («Аудит безопасности Intranet». С.А. Петренко. 2002 г.).

Универсальная услуга, которая может быть использована для повышения уровня ИБ компании. При этом, как показывает практика, разные компании по-разному представляют себе данный вид услуг.

<u>Аудит (контроль)</u> состояния защиты информации — специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

(Закон РФ «Об информации, информатизации и защите информации»)

составляющие аудита

способы проверки

средства проверки

результаты проверки

ЦЕЛЬ АУДИТА ИБ

- своевременно выявить существующие бреши и объективно оценить соответствие параметров, характеризующих режим информационной безопасности, необходимому уровню

ЭТИ ЗАДАЧИ ВЫПОЛНЯЮТ:

специальные организации аудиторов в области информационной безопасности. Они ставят своей целью проведение экспертизы соответствия системы информационной безопасности определенным требованиям, оценки системы управления безопасностью, повышения квалификации специалистов в области информационной безопасности.

(например, подразделения государственной технической комиссии при Президенте РФ или независимые, негосударственные организации)

Основные направления деятельности в области аудита безопасности информации

1. ***Аттестация объектов информатизации по требованиям безопасности информации.***

- аттестация автоматизированных систем, средств связи, обработки и передачи информации;
- аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
- аттестация технических средств, установленных в выделенных помещениях.

2. ***Контроль защищенности информации ограниченного доступа.***

- выявление технических каналов утечки информации и способов несанкционированного доступа к ней;
- контроль эффективности применяемых средств защиты информации.

продолжение

3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН)

- персональные ЭВМ, средства связи и обработки информации;

- локальные вычислительные системы;

- оформления результатов исследований в соответствии с требованиями Гостехкомиссии России.

4. Проектирование объектов в защищенном исполнении

- разработка концепции информационной безопасности (первая глава учебника);

- проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;

- проектирование помещений, предназначенных для ведения конфиденциальных переговоров.

Вопрос 2

Виды аудита информационной безопасности

КЛАССИФИКАЦИЯ УГРОЗ

Характер угрозы

Вид угрозы

Источник угрозы

Объект угрозы

АКТИВНЫЙ АУДИТ

- представляет исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий)

АКТИВНЫЙ АУДИТ

Суть активного аудита *состоит в том, что с помощью специального программного обеспечения (в том числе, с помощью систем анализа защищенности) и специальных методов осуществляется сбор информации о состоянии системы сетевой защиты.*

При осуществлении данного вида аудита на систему сетевой защиты моделируется как можно большее количество таких сетевых атак, которые может выполнить хакер.

Результатом активного аудита *является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информация, доступная любому потенциальному нарушителю) сети заказчика.*

По окончании активного аудита выдаются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить опасные уязвимости

Активный аудит делится «внешний» активный аудит и «внутренний» активный аудит

При **«внешнем» активном аудите** специалисты моделируют действия «внешнего» злоумышленника. В данном случае проводятся следующие процедуры:

- определение доступных из внешних сетей IP-адресов заказчика;
- сканирование данных адресов с целью определения работающих сервисов и служб, определение назначения отсканированных хостов;
- определение версий сервисов и служб сканируемых хостов;

изучение маршрутов прохождения трафика к хостам заказчика;

сбор информации об ИС заказчика из открытых источников;

- анализ полученных данных с целью выявления уязвимостей.

«Внутренний» активный аудит по составу работ аналогичен «Внешнему», однако при его проведении с помощью специальных программных средств моделируются действия «внутреннего» злоумышленника.

ЭКСПЕРТНЫЙ АУДИТ

представляет сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на следующем:

- требования, которые были предъявлены руководством в процессе проведения аудита;
- описание «идеальной» системы безопасности, основанное на аккумулированном в компании-аудиторе мировом и частном опыте.

ЭКСПЕРТНЫЙ АУДИТ СОСТОИТ:

- сбор исходных данных об информационной системе, об её функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных (с учетом ближайших перспектив развития);

- сбор информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализ;

- определение точек ответственности систем, устройств и серверов ИС;

- формирование перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков.

ЭТАПЫ ЭКСПЕРТНОГО АУДИТА

1. Анализ проекта информационной системы, топологии сети и технологии обработки информации, в ходе которого выявляются, например, такие недостатки существующей топологии сети, которые снижают уровень защищенности информационной системы.

2. Анализ информационных потоков организации. На данном этапе определяются типы информационных потоков ИС организации и составляется их диаграмма, где для каждого информационного потока указывается его ценность (в том числе ценность передаваемой информации) и используемые методы обеспечения безопасности, отражающие уровень защищенности информационного потока.

3. Анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам информационной безопасности.

АУДИТ НА СООТВЕТСТВИЕ СТАНДАРТАМ

- деятельность при которой информационная безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах

Причины проведения аудита на соответствие стандарту (и сертификации) можно условно разделить по степени обязательности данной услуги по отношению к компании:

-обязательная сертификация;

-сертификация, вызванная «внешними» объективными причинами;

-сертификация, позволяющая получить выгоды в долгосрочной перспективе;

- добровольная сертификация.

Основные стандарты, на соответствие которым проводится аудит системы информационной безопасности

существующие руководящие документы Гостехкомиссии:

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

- «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

- «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (ГОСТ Р ИСО/МЭК 15408-2002 или «Общие критерии»).

Зарубежные и международные стандарты:

- Международный стандарт ISO/IEC 17799 «Информационные технологии. Управление информационной безопасностью» (Information Technology — Information Security Management). На сегодняшний день является одним из самых распространенных и широко применяемым стандартом во всем мире.

- Международный стандарт WebTrust. Применим для подтверждения высокого уровня защищенности системы электронной коммерции и web-сервисов.

Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

-степень соответствия проверяемой информационной системы выбранным стандартам;

-степень соответствия собственным внутренним требованиям компании в области информационной безопасности;

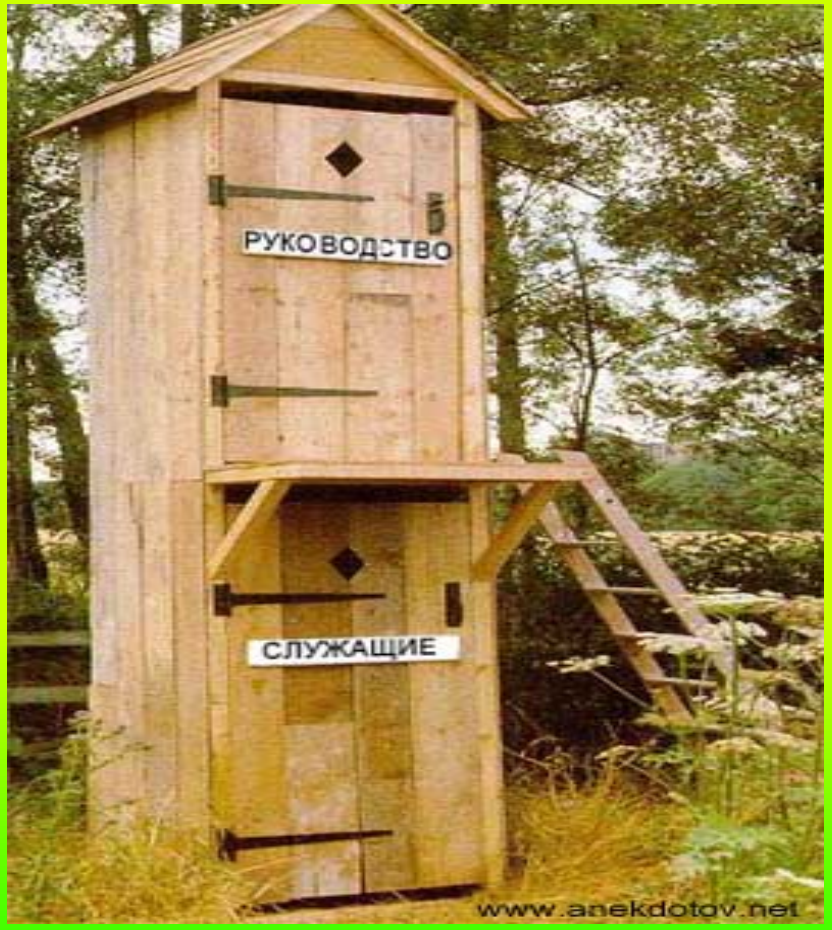
-количество и категории полученных несоответствий и замечаний;

-рекомендации по построению или модификации системы обеспечения информационной безопасности, позволяющие привести её в соответствие с рассматриваемым стандартом;

- подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании.

Вопрос 3

Аудит выделенных помещений



Аудит выделенных помещений представляет деятельность по выявлению средств несанкционированного съема информации и включает:

- подготовительный этап;
- этап непосредственного проведения аудита;
- заключительный этап.

Подготовительный этап аудита выделенных помещений:

- Уточнение границ и ранжирование по степени важности информации, относимой к конфиденциальной.

- Уточнение вероятного злоумышленника, оценка его возможностей, тактики внедрения средств НСИ и их использования.

ЭТАП НЕПОСРЕДСТВЕННОГО ПРОВЕДЕНИЯ АУДИТА

Предварительный осмотр объекта

1. Разработка перечня аппаратуры, необходимой для проведения проверки помещений и объектов.
2. Разработка дополнительных мер по активации внедренных средств НСИ на время проведения поиска с различными типами аппаратуры.
3. Распределение привлекаемых сил и средств по объектам и видам работ.
4. Уточнение частных методик использования привлекаемой аппаратуры в конкретных условиях проверки.
5. Оформление плана проведения комплексной проверки помещений и объектов и утверждение его у руководителя предприятия.
6. Подготовка аппаратуры для проведения поисковых и исследовательских работ.
7. Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых объектов и помещений.
8. Подготовка документов прикрытия работ по проверке помещений в соответствии с выбранной легендой прикрытия.
9. Подготовка бланков, схем, заготовок других документов, необходимых для проведения работ на последующих этапах.

Перечень специального оборудования и технических средств, рекомендуемых для проведения аудита помещений

Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2) — Визуальный осмотр оборудования, мебели, технологических коммуникаций.

Длина раздвижной штанги (с рукояткой), мм	550-1600
Масса носимого комплекта, кг	1.9
Масса рабочего комплекта, не более, кг	1.2
Размер сменных зеркал, мм	диам. 140, 80, 50, 35 - 110х65

Комплект луп, фонарей — Визуальный осмотр поверхностей и отверстий.

Комплект отверток, ключей и радиомонтажного инструмента — Разборка и сборка коммутационных, электроустановочных и других устройств и предметов.

Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus) — Визуальный осмотр труднодоступных полостей и каналов.

Гибкий технический эндоскоп серии «ЭТГ»

Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet) — Проверка предметов и элементов интерьера на наличие металлических включений.

Прибор нелинейный радиолокации (NR-900EM, ОРИОН NGE-400, РОДНИК 23) — Проверка строительных конструкций и предметов на наличие радиоэлектронных компонентов.

Описание NR-900EM Прибор нелинейной радиолокации

ОРИОН (NJE-4000)

- Переносный радиоприемник или магнитола — Озвучивание проверяемых помещений.

- Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможная замена по телефонным линиям: ТПУ-5К или SEL SP-18/T) — Проверка проводных коммуникаций на наличие нелинейности параметров линии.

Многофункциональный поисковый прибор (ПИРАНЬЯ, ПСЧ-5, D-008) — Проверка проводных коммуникаций на наличие информационных сигналов.

Прибор ST 031P "Пиранья"

СРМ-700
Зонд/монитор

Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000) —Анализ радиоэлектронной обстановки, выявление радиоизлучающих средств негласного съема информации.

Многозонный комплекс дистанционного радиомониторинга ST- 052

Крона Про Комплекс обнаружения радиоизлучающих средств и радиомониторинга

Удалённый модуль для ST-052

Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов) — Выявление радиоизлучающих видеокамер.

Обнаружитель скрытых видеокамер "Оптик"

Прибор «Амулет».

Обнаружитель скрытых видеокамер IRIS VCF-2000 PRO

Дозиметр поисковый (РМ-1401, НПО-3) — Обнаружение и локализация источников радиоактивного излучения.

"НОРКА" МИНИ, СТАНДАРТ, МАКСИ-Д, XL - переносная рентгенотелевизионная установка

установку ДЕЛЬТА

Портативная **рентгенотелевизионная установка** НОРКА...

Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА. ЗАРНИЦА) — Выявление информативных побочных электромагнитных излучений.

Навигатор-П2Г (Анализатор спектра E4402B ESA-E), 100 Гц - 3 ГГц.

"НАВИГАТОР"

Комплекс для проведения акустических и виброакустических измерений СПРУТ-4А — Выявление акустических и виброакустических сигналов и наводок, исследование звуко- и виброизоляции, проверка систем зашумления.

Виброакустический комплекс ВК-01

Комплекс для проведения акустических и виброакустических измерений "Спрут-6МА"

Структура плана аудита помещений:

- выводы из оценки противника;
- замысел проведения аудита помещений;
- целевая установка;
- перечень и краткая характеристика проверяемых помещений;
- перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований;
- время проведения проверки;
- легенда, под прикрытием которой будет проводиться проверка;
- меры по активации внедренных средств (несанкционированного съема информации (НСИ);
- действия в случае обнаружения средств НСИ;
- привлекаемые для проведения проверки силы, технические средства и их распределение по объектам и видам работ;
- основные особенности применения технических средств, определяемые условиями проверки;
- дополнительные меры по активизации внедренных средств НСИ;
- перечень подготавливаемых по результатам проверки итоговых и отчетных документов и срок их представления для утверждения.

Этапы непосредственного проведения аудита:

1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений.
2. Проверка элементов строительных конструкций, мебели и других предметов интерьера помещений с использованием специальных поисковых технических средств.
3. Выполнение запланированных мер по активации внедренных средств НСИ.

Проверка линий и оборудования проводных коммуникаций:

- линий силовой и осветительной электросети;
- линий и оборудования офисной и абонентской телефонной се
- линий селекторной связи;
- линий радиотрансляционной сети;
- линий пожарной и охранной сигнализации;
- линий системы часофикации и других проводных линий, в том числе, невыясненного назначения

Заключительный этап комплексной специальной проверки помещений

1. Обработка результатов исследования, оформление протоколов измерений, регистрационных журналов, проведение необходимых инженерных расчетов.
2. Определение технических характеристик, потребительских свойств изъятых средств НСИ, ориентировочного времени и способов их внедрения.
3. Составление описания проведенных работ и исследований с приложением необходимых схем и планов помещений.

Выводы

1. Аудит информационной безопасности фирмы — это мощное средство оценки состояния защиты информации.

2. Аудит может проводиться как собственными силами СБ фирмы, так силами специальных лицензированных аудиторских фирм.

3. Регулярность, периодичность и масштабность аудита определяются реальной обстановкой общей безопасности предприятия.