Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования «Казанский национальный исследовательский
технический университет им. А.Н. Туполева-КАИ»
Институт **Компьютерных технологий и защиты информации**

Кафедра **Компьютерных систем**

УТВЕРЖДАЮ
Ответственный за ОП
Верш И.С. Вершинин
«31» 08 2017 г.
Регистрационный номер 4010-17/н-059

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине

**Комплексные системы защиты информации**
(наименование дисциплины, практики)

Индекс по учебному плану: **Б1.В.ДВ.01.02**

Направление подготовки: **09.04.01 «Информатика и вычислительная техника»**

Квалификация: **магистр**

Магистерская программа: **Системное и сетевое администрирование (информатика как вторая компетенция)**

Виды профессиональной деятельности: **научно-исследовательская**

Заведующий кафедрой СИБ И.В. Аникин

Разработчик: доцент каф. СИБ Г.С. Корнилов

Казань 2017 г.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

**Комплексные системы защиты информации**

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению 09.04.01 «Информатика и вычислительная техника», учебному плану специальности 09.04.01 «Информатика и вычислительная техника». Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Комплексные системы защиты информации». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника». В составе ФОС присутствуют оценочные средства в виде тестовых заданий и контрольных вопросов различного уровня сложности, которые позволяют провести оценку порогового, продвинутого и превосходного уровней освоения компетенций по дисциплине.

ФОС обладают необходимой степенью приближенности к задачам будущей профессиональной деятельности обучающихся, связанным с применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и ин-формационных технологий (ПК-7). Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методической комиссии института КТЗИ от «31» августа 2017 г., протокол № 8.

Председатель УМК института КТЗИ _____ В.В. Родионов

## Содержание

**Введение**

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Комплексные системы защиты информации» – это комплект методических и контрольно-измерительных материалов, предназначенных для определения уровня сформированности компетенций, оценивания знаний, умений, владений на разных этапах освоения дисциплины для проведения промежуточной аттестации обучающихся по дисциплине.

ФОС ПА является составной частью учебного и методического обеспечения программы магистратуры по направлению 09.04.01 «Информатика и вычислительная техника».

Задачи ФОС по дисциплине «Комплексные системы защиты информации»:

– оценка запланированных результатов освоения дисциплины обучающимися в процессе изучения дисциплины, в соответствии с разработанными и принятыми критериями по каждому виду контроля;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков и формирования компетенций, определенных в ФГОС ВО по направлению подготовки

ФОС ПА по дисциплине «Комплексные системы защиты информации» сформирован на основе следующих основных принципов оценивания:

– пригодности (валидности) (объекты оценки соответствуют поставленным целям обучения);

– надежности (использования единообразных стандартов и критериев для оценивания запланированных результатов);

– эффективности (соответствия результатов деятельности поставленным задачам).

ФОС ПА по дисциплине «Комплексные системы защиты информации» разработан в соответствии с требованиями ФГОС ВО по направлению 09.04.01 «Информатика и вычислительная техника» для аттестации обучающихся на соответствие их персональных достижений требованиям поэтапного

формирования соответствующих составляющих компетенций и включает контрольные вопросы (или тесты) и типовые задания, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций.

## 1. Формы промежуточной аттестации по дисциплине

Дисциплина «Комплексные системы защиты информации» изучается в 3 семестре при очной форме обучения и завершается промежуточной аттестацией в форме экзамена.

## 2. Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации по дисциплине «Комплексные системы защиты информации» при очной форме обучения.

Таблица 1

Оценочные средств для промежуточной аттестации

(очная форма обучения)

| № п/п | Семестр | Форма промежуточной аттестации | Оценочные средства |
|---|---|---|---|
| 1. | 3 | Экзамен | ФОС ПА |

## 3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Перечень компетенций и их составляющих, которые должны быть сформированы при изучении темы соответствующего раздела дисциплины «Комплексные системы защиты информации», представлен в таблице 2.

Таблица 2

Перечень компетенций и этапы их формирования
в процессе освоения дисциплины

| № п/п | Этап формирования (семестр) | Наименование раздела | Код формируемой компетенции (составляющей компетенции) | | Форма промежуточной аттестации |
|---|---|---|---|---|---|
| 1. | 3 | Сущность и задачи комплексной системы защи-ты информации. Общие принципы проектирования КСЗИ | ПК-7 | ПК-7.З | Экзамен |
| 2. | 3 | Международная практика проектирования КСЗИ. Построение процессов системы управления информационной безопасности | ПК-7 | ПК-7.З<br>ПК-7.В | Экзамен |
| 3. | 3 | Российская практика построения проблемно-ориентированных КСЗИ. Аудит информационной безопасности. Оценка эффективности КСЗИ | ПК-7 | ПК-7.З<br>ПК-7.У<br>ПК-7.В | Экзамен |

## 4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкалы оценивания

Показатели и критерии оценивания сформированности компетенций на экзамене, приведены в таблице 3.

Таблица 3

Показатели и критерии оценивания сформированности компетенций на экзамене

| № п/п | Этап формирования (семестр) | Код формируемой компетенции (составляющей компетенции) | | Критерии оценивания | Показатели оценивания (планируемые результаты обучения) | | |
|---|---|---|---|---|---|---|---|
| | | | | | Пороговый уровень | Продвинутый уровень | Превосходный уровень |
| 1. | 3 | ПК-7.3 | ПК-7.3 | Теоретические навыки | Знание требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем<br>Знание отдельных технических средств КСЗИ, используемых для защиты информации объектов информатизации<br>- Знание одного из технических средств КСЗИ, используемых для аудита информационной безопасности<br>- практически применять основные программные средства КСЗИ защиты ин- | - Знание основных сертифицированных ФСТЭК технических средств КСЗИ, используемых для защиты информации в реальном секторе экономики<br>- Знание нескольких разнотипных технических средств КСЗИ, используемых для активного и пассивного исследования ТКУИ/НСД для одной из отраслей экономики<br>- Умение практически применять и конфигурировать в соответствии с требованиями внутренние механизмы защиты в реальном секторе экономики для операционных систем<br>- Умение практически | - Знание основных сертифицированных ФСТЭК технических средств КСЗИ, используемых для защиты информации в реальном секторе экономики в различных ТСПИ<br>- Знание технических средств КСЗИ, используемых для обхода механизмов противодействия активному и пассивному исследованию ТКУИ/НСД<br>- Умение практически применять и конфигурировать в соответствии с требованиями внутренние механизмы защиты в реальном секторе экономики для операционных систем и СЗИ ТКУИ/НСД, серти- |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | формации в реальном секторе экномики<br>- практически разрабатывать проекты документов, регламентирующих работу но обеспечению информационной безопасности<br>- Умение практически применять внутренние механизмы защиты в реальном секторе экномики для операционных систем<br>- Умение практически применять одно из технических средств КСЗИ, используемых для активного и пассивного исследования ТКУИ/НСД | применять несколько разнотипных технических средств КСЗИ, используемых для активного и пассивного исследования ТКУИ/НСД для одной из отраслей экономики | фицированных ФСТЭК<br>- Умение описывать алгоритм функционирования на основе активного и пассивного исследования электромагнитного излучения |
| 2. | 3 | ПК-7 | ПК-7.З<br>ПК-7.У<br>ПК-7.В | Практические навыки | - навыками аудита документов, регламентирующих работу по обеспечению информационной безопасности | Владение навыками аудита документов, регламентирующих работу по обеспечению информационной безопасности в государственной системе ЗИ | Владение навыками аудита документов, регламентирующих работу по обеспечению информационной безопасности в государственной и международной системе ЗИ |

Формирование оценки при промежуточной аттестации по итогам освоения дисциплины зависит от уровня освоения компетенций, которые обучающийся должен освоить по данной дисциплине. Связь между итоговой оценкой и уровнем освоения компетенций (шкала оценивания) представлена в таблице 4.

Таблица 4

Описание шкалы оценивания

| Шкала оценивания | | Описание оценки в требованиях к уровню и объему компетенций |
|---|---|---|
| Словесное выражение | Выражение в баллах | |
| Отлично | от 86 до 100 | Освоен **превосходный** уровень всех компетенций (составляющих компетенций) |
| Хорошо | от 71 до 85 | Освоен **продвинутый** уровень всех компетенций (составляющих компетенций) |
| Удовлетворительно | от 51 до 70 | Освоен **пороговый** уровень всех компетенций (составляющих компетенций) |
| Неудовлетворительно | до 51 | Не освоен **пороговый** уровень всех компетенций (составляющих компетенций) |

## 5. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формирование оценки по результатам текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Комплексные системы защиты информации» приведено в таблице 5.

Таблица 5

Формирование оценки по итогам освоения дисциплины

| Наименование контрольного мероприятия | Рейтинговые показатели | | | | |
|---|---|---|---|---|---|
| | I аттестация | II аттестация | III аттестация | по результатам текущего контро-ля | по итогам промежуточной аттестации (зачета /экзамена) |
| **Раздел 1.** *Сущность и задачи ком-плексной системы защиты информации. Общие принципы проектирования КСЗИ* | **10** | | | **10** | |
| Тест текущего контроля по разделу | 10 | | | 10 | |
| **Раздел 2.** *Международная практика проектирования КСЗИ. Построение процессов системы управления информационной безопасности* | | **20** | | **20** | |
| Тест текущего контроля по разделу | | 10 | | 10 | |
| Защита лабораторных работ | | 10 | | 10 | |
| **Раздел 3.** *Российская практика построения проблемно-ориентированных КСЗИ. Аудит информационной безопасности. Оценка эффективности КСЗИ* | | | **20** | **20** | |
| Тест текущего контроля по разделу | | | 10 | 10 | |
| Защита лабораторных работ | | | 10 | 10 | |
| **Промежуточная аттестация (зачет):** | | | | | **50** |
| – тест промежуточной аттестации по дисциплине | | | | | 20 |
| – ответы на контрольные вопросы в письменной форме | | | | | 30 |

## 6. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

### 6.1. Тестовые задания

---

# 1.

Что из перечисленного относится к основным принципам построения КСЗИ?

- ❑ системность, комплексность, непрерывность защиты
- ❑ разумная достаточность, гибкость управления и применения
- ❑ открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств
- ■ все из перечисленного

---

# 2.

Укажите правильную последовательность этапов разработки КСЗИ.

- ❑ проектирование системы защиты информации; внедрение системы защиты информации; сопровождение системы информационной безопасности
- ❑ обследование организации; проектирование системы защиты информации; внедрение системы защиты информации; сопровождение системы информационной безопасности;
- ❑ обследование организации; проектирование системы защиты информации; внедрение системы защиты информации; обучение специалистов по защите информации;
- ■ обследование организации; проектирование системы защиты информации; внедрение системы защиты информации; сопровождение системы информационной безопасности; бучение специалистов по защите информации;

---

# 3.

Какие существуют группы факторов влияющих на защиту информации?

- ❑ внутренние и внешние факторы
- ■ субъективные и объективные факторы
- ❑ внутренние: субъективные и объективные; внешние: субъективные и объективные
- ❑ технические и финансовые факторы

---

# 4.

Что из перечисленного является способами защиты информации?

- ❑ препятствие, управление, маскировка
- ❑ регламентация, принуждение, побуждение
- ■ препятствие, управление, маскировка, регламентация, принуждение, побуждение
- ❑ регламентация, препятствие, маскировка

## 5.

Что из перечисленного не является средствами защиты информации?

- ❑ физические
- ❑ программные
- ❑ морально-этические
- ■ психологические

## 6.

Что из перечисленного не является свойством информации с точки зрения защиты?

- ❑ конфиденциальность
- ❑ доступность
- ❑ целостность
- ■ достоверность

## 7.

Какие критерии не используются при определении конфиденциальности информации?

- ❑ ценность информации
- ❑ длительность жизненного цикла информации
- ■ объемы информации
- ❑ возможности предприятия и вид деятельности

## 8.

Что является объектом защиты?

- ❑ аппаратные средства
- ❑ программные средства
- ❑ информационное обеспечение
- ■ все из перечисленного

## 9.

Что является видами угроз информационной безопасности?

❑ ошибки эксплуатации, преднамеренные действия нарушителей и злоумышленников

❑ стихийные бедствия и аварии, сбои и отказы оборудования, последствия ошибок проектирования и разработки компонентов автоматизированных систем,

■ стихийные бедствия и аварии, сбои и отказы оборудования, последствия ошибок проектирования и разработки компонентов автоматизированных систем, ошибки эксплуатации, преднамеренные действия нарушителей и злоумышленников

## 10.

Какая совокупность определяет понятие «Атака»

❑ Источник угрозы ИБ и метод реализации угрозы

■ Источник угрозы ИБ, уязвимость и метод реализации угрозы

❑ уязвимость и метод реализации угрозы

## 11.

Что из перечисленного не является методом реализации угрозы ИБ?

■ стихийный

❑ аналитический

❑ социальный

❑ организационный

## 12.

Что из перечисленного не является источником угрозы ИБ?

❑ антропогенные источники

■ случайные источники

❑ стихийные

❑ техногенные источники

## 13.

Какие существуют классы уязвимостей?

☑ объективные

❑ программные

☑ субъективные

☑ случайные

❑ аппаратные

## 14.

При разработке модели нарушителя определяются:

☑ предположения о категориях лиц, к которым может принадлежать нарушитель

☑ предположения о мотивах действий нарушителя
☑ предположения о квалификации нарушителя и его технической оснащенности
☑ ограничения и предположения о характере возможных действий нарушителей

## 15.

По отношению к АС нарушители могут быть:

■ внутренними и внешними
❑ субъективными и объективными
❑ осведомленными и неосведомленными
❑ все из перечисленного

## 16.

Что не относится к классификации нарушителей?

❑ уровень знаний, время действия, место действия
❑ уровень возможностей
■ уровень доступа

## 17.

Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним это:

❑ утечка
❑ несанкционированный доступ
■ разглашение

## 18.

Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена это:

■ утечка
❑ несанкционированный доступ
❑ разглашение

## 19.

Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам это:

❑ утечка
■ несанкционированный доступ
❑ разглашение

## 20.

На какие группы по способу получения информации можно разделить потенциальные каналы доступа?

- ❑ В течение одной минуты
- ❑ В течение одного сеанса аутентификации
- ■ Физические, электромагнитные, информационные

## 21.

На какие классы по способам осуществления подразделяются все меры (компоненты) обеспечения безопасности компьютерных систем?

- ☑ Правовые
- ☑ Морально-этические
- ☑ оргаизационные
- ☑ физические
- ☑ технические

## 22.

Какое из наименований не является типом модели управления доступом?

- ❑ Модель конечного автомат
- ■ Модель приоритетов
- ❑ Модель информационных потоков
- ❑ Модель интерференции

## 23.

Какие группы сотрудников подразумевает кадровое обеспечение КСЗИ?

- ❑ программист, администратор безопасности системы, администратор безопасности данных, руководитель группы
- ❑ оператор, программист, администратор безопасности системы, руководитель группы
- ■ сотрудник группы безопасности, администратор безопасности системы, администратор безопасности данных, руководитель группы

## 24.

Какое из наименований не относится к техническим каналам утечки?

- ❑ акустический
- ❑ оптический
- ❑ радиоэлектронный
- ■ программно-аппаратный
- ❑ материаьно-вещественный

## 25.

Укажите правильную последовательность этапов проектирования КСЗИ?

❑ разработка технического задания, эскизное проектирование, техническое проектирование, рабочее проектирование, тестирование, производство опытного образца
❑ разработка технического задания, техническое проектирование, производство опытного образца
■ разработка технического задания, эскизное проектирование, техническое проектирование, рабочее проектирование, производство опытного образца

## 26.

Деятельность в терминах процессного подхода можно представить в виде совокупности следующих трёх групп высокоуровневых процессов:

☑ процессы управления организацией
☑ основные процессы (основной деятельности)
☑ вспомогательные процессы
❑ дополнительные процессы
❑ условные процессы

## 27.

Аббревиатура PDSA означает:

❑ Созидай, выполняй, контролируй
❑ Планируй, проверяй, изменяй
■ Планируй, делай, изучай, действуй
❑ Изучай, планируй, делай, проверяй

## 28.

ITIL это:

❑ Стандарт качества
■ Библиотека ИТ-инфраструктуры
❑ Стандарт безопасности
❑ Библиотека управления безопасностью

## 29.

ITIL содержит рекомендации:

■ По управлению ИТ-сервисами
❑ По управлению информационной безопасностью
❑ По управлению проектированием

## 30.

В процессной модели ITIL выделяются следующие группы процессов управления ИТ:

- ☑ на уровне инфраструктуры
- ☑ на уровне поддержки услуг
- ☑ на уровне предоставления услуг
- ❑ на уровне обеспечения безопасности

## 31.

Модель уровней зрелости предприятий CMMI выделяет:

- ❑ 3 уровня зрелости
- ❑ 10 уровней зрелости
- ■ 5 уровней зрелости
- ❑ 7 уровней зрелости

## 32.

Для того чтобы внедряемые лучшие практики (CobiT, ITIL, ISO) были эффективными, необходимо следовать следующим правилам:

- ❑ Систематизация
- ❑ Масштабируемость
- ☑ Конкретизация
- ☑ Приоретизация
- ☑ Планирование
- ☑ Избежание известных проблем
- ☑ Внедрение передового опыта

## 33.

Microsoft System Center это:

- ❑ Набор правил разграничения доступа Microsoft
- ❑ Модель управления доступом Microsoft
- ■ Инструментарий MSM (Microsoft Solutions for Management)
- ❑ Инструментарий MOF (Microsoft Operations Framework)

## 34.

Модель MOF содержит следующие квадранты:

- ☑ изменения
- ☑ эксплуатации
- ☑ поддержки
- ☑ оптимизации
- ❑ проектирования

## 35.

Основные структуры ГОСТ Р ИСО 15408 это:

- ☑ Профиль защиты
- ☑ Задание безопасности
- ❑ Модель управления
- ❑ Модель проектирования

## 36.

Варианты технических решений восстановления деятельности после бедствия:

- ☑ Использование «горячего» резерва
- ☑ Использование «холодного» резерва
- ☑ Использование внутренних резервов
- ☑ Заключение соглашений
- ❑ Использование виртуальных резервов

## 37.

Какие органы государственной власти уполномочены осуществлять контроль и надзор за обеспечением безопасности ПДн:

- ❑ Министерство связи
- ☑ ФСТЭК России
- ☑ ФСБ России
- ☑ Роскомнадзор России

## 38.

Классификация ИСПДн возложена:

- ❑ На Роскомнадзор России
- ❑ На ФСТЭК России
- ■ На ФСБ России
- ❑ На минсвязи России

## 39.

Правила классификации ИСПДн включают следующие этапы:

- ☑ Сбор и анализ исходных данных по информационной системе
- ☑ Присвоение информационной системе соответствующего класса
- ☑ Документальное оформление акта классификации информационной системы
- ❑ Тестирование
- ❑ Контроль

## 40.

Количество категорий ПДн в соответствии с руководящими документами по обеспечению безопасности ПДн:

- ❑ 2
- ❑ 6
- ■ 4
- ❑ 5

## 41.

Количество классов ИСПДн в соответствии с руководящими документами по обеспечению безопасности ПДн:

- ❑ 2
- ❑ 6
- ■ 4
- ❑ 5

## 42.

Частная модель угроз строится на основе:

- ❑ Модели скрытых угроз
- ■ Базовой модели угроз

## 43.

Построение системы менеджмента защиты информации банка может быть построено на основе:

- ❑ Стандарта ISO 9001
- ❑ Стандарта PCI DSS
- ■ Стандарта СТО БР ИББС ЦБ России

## 44.

Проект по созданию СМЗИ в банковской организации, в соответствии со стандартом ЦБ, включает следующие этапы:

- ❑ Обследование СМЗИ, планирование, реализация и эксплуатация, мониторинг и анализ, совершенствование
- ■ Планирование СМЗИ, реализация и эксплуатация, мониторинг и анализ, совершенствование

## 45.

PCI DSS включает следующие группы требований:

- ❑ Защита данных платежных карт, реализация программы управления уязвимостями, реализация мер по строгому контролю доступа, регулярный мониторинг и тестирование сетей

❑ Предварительные, основные, дополнительные

■ Построение и поддержание защищенной сети, защита данных платежных карт, реализация программы управления уязвимостями, реализация мер по строгому контролю доступа, регулярный мониторинг и тестирование сетей, поддержание политики информационной безопасности

❑ Технические, организационные, правовые, социальные

## 46.

Какие существуют подходы к оценке эффективности КСЗИ?

☑ Классический

☑ Официальный

❑ Упреждающий

☑ Экспериментальный

❑ Мысленный

## 47.

Сколько классов защищенности СВТ согласно руководящему документу ФСТЭК России?

❑ 3

❑ 5

■ 6

❑ 7

## 48.

Сколько классов защищенности АС согласно руководящему документу ФСТЭК России?

❑ 3

❑ 5

■ 9

❑ 10

## 49.

На чем основан официальный подход оценки эффективности СУИБ?

❑ На процедуре декларации соответствия

❑ На процедуре удаленного контроля

■ На процедуре сертификации

❑ На процессе активного аудита

## 50.

Что понимается под аудитом информационной безопасности?

❑ проверка правильности оформления расходования средств на обеспечение информационной безопасности

■ системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности на всех основных уровнях обеспечения безопасности

❑ обеспечение записи действий пользователей в корпоративной сети

## 51.

Какие задачи решает аудит ИБ?

☑ защитить информацию от умышленного искажения (разрушения), несанкционированного копирования, доступа или использования;

☑ обеспечить контроль действий пользователей в корпоративной сети предприятия;

☑ своевременно оценить и переоценить информационные риски бизнес-деятельности компании;

☑ выработать оптимальные планы развития и управления предприятием.

☑ получить объективную и независимую оценку текущего состояния защищенности информационных ресурсов.

❑ проверка правильности использования пожарных систем

## 52.

Какие задачи решает аудит ИБ?

☑ защитить информацию от умышленного искажения (разрушения), несанкционированного копирования, доступа или использования;

☑ обеспечить контроль действий пользователей в корпоративной сети предприятия;

☑ своевременно оценить и переоценить информационные риски бизнес-деятельности компании;

☑ выработать оптимальные планы развития и управления предприятием.

☑ получить объективную и независимую оценку текущего состояния защищенности информационных ресурсов.

❑ проверка правильности использования пожарных систем

## 53.

Какие варианты проведения аудита существуют?

☑ Комплексный аудит

❑ Сверочный

❑ Измерительный

☑ Точечный

☑ Периодичный

☑ Проверочный

❑ Почасовой

## 54.

Какие виды работ не входят в аудит ИБ?

❑ Организационно-технологический анализ ИС предприятия.
❑ Экспертиза решений и проектов.
❑ Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации.
☑ Специсследования и спецпроверки
❑ Работы, поддерживающие практическую реализацию плана защиты.
❑ Повышение квалификации и переподготовка специалистов.
❑ Сопровождение системы информационной безопасности после проведенного комплексного анализа или анализа элементов системы ИБ предприятия.
❑ Ежегодная переоценка состояния ИБ.

## 55.

Какой вид аудита целесообразно провести при смене администратора вычислительной сети?

❑ Комплексный аудит
❑ Точечный
☑ Проверочный
❑ Периодичный

## 56.

Какие способы выбора показателей защищенности информации вы знаете?

☑ определение минимального набора необходимых для защиты информации функций, соответствующего конкретному классу защищенности в соответствии с принятыми стандартами, например существующими руководящими документами ФСТЭК РФ;
☑ определение профиля защиты, в котором учитываются особенности решения задач защиты информации на предприятии (в соответствии с международными стандартами ISO15408, ISO 17799, 27001, германским стандартом BSI).
❑ Определение матрицы доступа с иерархическими правилами разграничения доступа

## 57.

В чем заключается методология проведения аудита ИБ?

☑ анализ требований к корпоративной системе информационной безопасности;

☑ инструментальные проверки состояния информационной безопасности предприятия;
☑ анализ информационных рисков предприятия.
❑ финансовые проверки бухгалтерии

## 58.

Какие сертифицированные средства инструментальной проверки вы знаете

☑ Xspider,
❑ Cobra
☑ Internet Scanner
☑ System Security Scanner,
☑ NetRecon,
☑ Cisco Secure Scanner
❑ RiskManager

## 59.

Что такое профиль защиты?

☑ функционально полный, прошедший апробацию, стандартизованный набор требований, предназначенный для многократного использования.
❑ полная комбинация требований, являющихся необходимыми для создания и оценки ИБ конкретной системы или продукта ИТ

## 60.

Что такое задание по безопасности?

❑ функционально полный, прошедший апробацию, стандартизованный набор требований, предназначенный для многократного использования.
☑ полная комбинация требований, являющихся необходимыми для создания и оценки ИБ конкретной системы или продукта ИТ

## 61.

Каких признаков классификации видов и способов аудита ИБ не существует?

❑ По масштабу
❑ По характеру
☑ По компетенции привлекаемых специалистов
❑ В зависимости от стадии жизненного цикла ИС организации
❑ По глубине
❑ По виду выполняемых работ

## 62.

Какие основные методики аудита вы знаете?

☑ Аудит на основе ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
❑ Аудит на основе ГОСТ Р 51583
☑ Аудит ИБ на основе банковских стандартов Банка России (СТО БР ИББС-1.0-2006).
☑ Аудит ИБ на основе стандартов ISO 17799 и ISO 27001.
❑ Аудит на основе BS 25999
☑ Аудит ИБ на основе национального стандарта США NIST 800-53 «Recommended Security Controls for Federal Information Systems».
☑ Аудит ИБ на основе стандарта COBIT.

# 63.

Как устанавливается значимость каждого требования стандарта ISO/IEC 17799 в программном продукте «Кондор»?

☑ Значимость каждого требования стандарта ISO/IEC 17799 устанавливается на основе экспертных оценок в виде коэффициента от 1 до 100 в зависимости от степени влияния требования на информационную систему организации
❑ Значимость каждого требования стандарта ISO/IEC 17799 устанавливается на основе экспертных оценок в виде коэффициента от 1 до 1000 в зависимости от степени влияния требования на информационную систему организации
❑ Значимость каждого требования стандарта ISO/IEC 17799 устанавливается на основе экспертных оценок в виде коэффициента от 1 до 100000 в зависимости от степени влияния требования на информационную систему организации

# 64.

Перечислите основные международные и национальные стандарты оценки и управления информационной безопасностью

❑ ASD
☑ ISO 15408,
☑ ISO 17799 (BS 7799),
❑ ISO 51285
☑ ISO 27001,
☑ ISO 27002
☑ BSI;
☑ COBIT,
❑ ISO 27512
☑ SAC,
☑ COSO,
☑ SAS 55/78

## 65.

Какие вопросы из нижеперечисленных рассматривает стандарт ISO/IEC 17799:2005 (BS 7799/1:2005)

☑ требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
☑ управление бизнес/процессами компании с точки зрения информационной безопасности;
☑ внутренний аудит информационной безопасности компании.
❑ спецификации управляющих процессов и возможный инструментарий (Control Objectives)

## 66.

В какой части COBIT 3rd Edition рассматриваются рекомендации по выполнению аудита компьютерных информационных систем (Audit Guidelines).

❑ В первой
❑ Во второй
❑ В третьей
☑ В четвертой

## 67.

Какие приказы по ИБ оформляются в организации?

☑ на проведение работ по защите информации;
❑ на посещение предприятия контрагентами
☑ о назначении лиц, ответственных за эксплуатацию объекта информатизации;
☑ на обработку в АС (обсуждение в ЗП) конфиденциальной информации.

## 68.

Носители информации на магнитной, оптической и бумажной основе должны в подразделениях организаций в установленном порядке.

☑ учитываться, храниться и уничтожаться
❑ обрабатываться, передаваться и приниматься
❑ получаться и уничтожаться

## 69.

Кто может находиться в помещениях где размещаются ОТСС в период обработки конфиденциальной информации?

❑ все лица имеющие нужный уровень допуска

☑ лица, допущенные в установленном порядке к обрабатываемой информации

## 70.

Какие стадии жизненного цикла проходит ИТ в модели COBIT?

☑ Планирование и организация работы.
☑ Приобретение и ввод в действие.
❑ Налаживание энергоснабжения
☑ Поставка и поддержка.
❑ Проверка настроек
☑ Мониторинг.

## 71.

Чем определены требования к перечню защищаемых помещений?

☑ п. 4.2.1 СТР-К
❑ п. 4.2.4. СТР-К
❑ п. 3.5.1 СТР-К

## 72.

Чем регламентируется обязательность наличия в организации «Инструкция по организации доступа во внешние сети (Интернет) пользователей КИС и выделенных АРМ»?

❑ п.4.3.1 СТР-К
☑ п.6.3.6 СТР-К
❑ п.8.4.5 СТР-К

## 73.

Чем определяется список ресурсов, подлежащих резервному копированию?

☑ ГОСТ Р ИСО/МЭК 17799
❑ ГОСТ Р ИСО/МЭК 27001
❑ ГОСТ Р ИСО/МЭК 27005

## 74.

Чем регламентируется инструкция по организации доступа во внешние сети (Интернет) пользователей КИС и выделенных АРМ

❑ п.4.3.1 СТР-К
☑ п.6.3.6 СТР-К
❑ п.8.4.5 СТР-К

## 75.

Какие объекты информатизации подлежат обязательной аттестации?

- ☑ ОИ, предназначенные для обработки информации, составляющей гостайну,
- ☑ ОИ предназначенные для управления экологически опасными объектами,
- ☑ Объекты предназначенные для ведения секретных переговоров.
- ❑ ОИ предназначенные для обслуживания совета директоров

## 76.

Что подтверждается при аттестации ОИ?

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации:

- ☑ от несанкционированного доступа, в том числе от компьютерных вирусов;
- ❑ от модификации данных и программ
- ❑ от нарушений доступности серверов различного назначения
- ☑ от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное облучение, электромагнитное и радиационное воздействие);
- ☑ от утечки или воздействия на нее за счет специальных устройств, встроенных в объект информатизации.

## 77.

Что обычно выступает в качестве источников угроз нарушения целостности информации (выберите правильные)

- ☑ случайные или преднамеренные критические ситуации в системе
- ☑ вирусы
- ❑ подбор пароля
- ☑ "троянские кони"
- ☑ программные закладки.
- ❑ несанкционированное вскрытие помещения администраторов

## 78.

Кто, как правило, осуществляет контроль за выполнением положений политики аудита?

- ☑ отдел информационной защиты службы безопасности.
- ❑ председатель координационного совета по ИБ
- ❑ начальник службы безопасности

## 79.

Кто оплачивает расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации?

- ☑ Заявители
- ❑ Орган по аттестации
- ❑ Аккредитованный орган ФСТЭК
- ❑ Центр по сертификации

Чем определяются области контроля при проведении аудита ИБ?

- ❑ Положениями международных стандартов в области ИБ
- ☑ списками контроля утвержденными в Компании
- ❑ руководящими документами ФСТЭК

## 80.

Каково наиболее серьезное нарушение управления учетными записями?

- ☑ Не отключены все неиспользуемые встроенные учетные записи.
- ❑ Ослабленные пароли
- ❑ Не установлены средства шифрования информации

## 81.

Что должно производиться в случае нарушения целостности объекта ОС?

- ☑ автоматическое восстановление эталонного состояния
- ☑ регистрация в журнале событий
- ❑ отправление сообщения Microsoft
- ☑ рассылка уведомлений
- ☑ запрет загрузки/останов ОС

## 82.

Какие виды обследования вы знаете?

- ❑ визуальное
- ❑ документальное
- ☑ информационное
- ☑ инструментальное

## 83.

Перечислите документацию подлежащую проверке?

- ☑ нормативная,
- ❑ бухгалтерская
- ☑ распорядительная
- ☑ рабочая документации

❑ организационная

## 84.

За что отвечает владелец аттестованного объекта информатизации?

☑ за выполнение установленных условий функционирования объекта информатизации
❑ за периодическое изменение правил обработки информации
☑ за выполнение технологии обработки защищаемой информации
☑ за выполнение требований по безопасности информации

## 85.

В каком случае «Аттестат соответствия» не выдается?

☑ При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией
❑ При задержке оплаты работы аттестационной комиссии
❑ При несогласии с правилами проведения аттестования

## 86.

Куда имеет право обратиться заявитель в случае несогласия с отказом в выдаче "Аттестата соответствия"

❑ в ФСБ
☑ в ФСТЭК РФ
❑ в МО РФ

## 87.

Кем определяется состав нормативной и методической документации для аттестации?

☑ органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.
❑ органом по сертификации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.
❑ Аттестуемой организацией.

## 88.

Перечислите средства автоматизации анализа рисков

☑ RiskPAC (CSCI);
☑ CRAMM (Великобритания);

- ☑ MARION(Франция);
- ❑ MBSA (США)
- ☑ RiskWatch (США);
- ☑ Авангард (ИСА РАН, Россия);
- ☑ ГРИФ (Россия).
- ❑ Xspider (Россия)

## 89.

Какие сканеры вы знаете?

- ❑ NetView
- ☑ ISS Internet Scanner 6.2.1
- ☑ XSpider 8.0
- ❑ Oberon
- ☑ LanGuard 2.0
- ☑ ShadowSecurityScanner 5.31
- ☑ XFocus X-Scan v1.3 GUI

## 90.

Какой сканер имеет сертификат ФСТЭК?

- ❑ ISS Internet Scanner 6.2.1
- ☑ XSpider 8.0
- ❑ LanGuard 2.0
- ❑ ShadowSecurityScanner 5.31
- ❑ XFocus X-Scan v1.3 GUI

## 91.

Какие «бреши» в защите может обнаружить САЗ?

- ☑ наличие вредоносного ПО (в частности, вирусов),
- ❑ наличие аппаратных закладок
- ☑ слабые пароли пользователей,
- ☑ неудачно сконфигурированные операционные системы,
- ☑ небезопасные сетевые сервисы,
- ❑ неисправности IDS/IPS
- ☑ неустановленные заплаты,
- ☑ уязвимости в приложениях

## 92.

Относятся ли антивирусные пакеты к САЗ?

- ☑ Да
- ❑ Нет

# 93.

Что является основной задачей аудитора?

❑ решение о внедрении в систему новых механизмов безопасности и модификации старых

☑ обоснование рекомендуемых контрмер для руководства организации

**Оценка практических умений и навыков:**

Составление перечня сведений, составляющих коммерческую тайну предприятия.

Анализ сведений, подлежащих рассмотрению

Оценка возможного ущерба предприятию

Проверка рассматриваемых сведений на общеизвестность или общедоступность

Проверка предприятия на осуществление надлежащих мер по сохранению конфиденциальности рассматриваемых сведений

Проверка рассматриваемых сведений на государственную секретность и на защиту авторским и патентным правом

Проверка сведений на общедоступность и на способность нанести ущерб

Составление перечня персональных данных на предприятии

Определение классов защищенности объектов информатизации и выделенных помещений предприятия

Классификация автоматизированных систем обработки информации

Требования по защите информации от НСД для АС

Определение класса защищенности для АС, в которой обрабатывается государственная тайна

Определение требуемой категории выделенного помещения

Определение класса защищенности для АС, в которой обрабатывается коммерческая тайна

Классификация информационной системы обработки персональных данных

Анализ информации с точки зрения необходимости ее защиты

Оценка эффективности принятых мероприятий по защите информации ограниченного доступа

Методы работы с персоналом и их характеристика

Мотивация деятельности персонала

Форирование акта классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации

### 6.2. Контрольные вопросы

1. Дайте определение понятию комплексная система защиты информации.
2. На что направлена КСЗИ? каковы ее цели и задачи?
3. Какие существуют уровни мер защиты?
4. Перечислите принципы организации КСЗИ.
5. Перечислите этапы разработки КСЗИ.
6. Перечислите уровни Политики безопасности и их состав.
7. Перечислите состав логической цепочки, лежащей в основе моделирования процессов нарушения информационной безопасности.
8. Приведите примеры объективных уязвимостей.
9. Приведите примеры субъективных уязвимостей.
10. Приведите примеры случайных уязвимостей.
11. Перечислите типы источников угроз.
12. Какие существуют методы реализации угроз?
13. Какие существуют потенциальные каналы и методы несанкционированного доступа к информации?
14. Какие роли (должности), как правило, должны быть созданы для кадрового обеспечения функционирования КСЗИ?
15. Что должна отражать модель нарушителя?
16. Перечислите существующие виды обеспечения КСЗИ.
17. Дайте определение понятию «процесс». Какова цель процессного подхода?
18. Какие преимущества имеет процессный подход?
19. Что представляет собой цикл Деминга и модель PDSA?
20. Какова связь между циклом Деминга и библиотекой ITIL?
21. Какие группы процессов выделяет ITIL?
22. Какие принципы лежат в основе ITSM?
23. Перечислите уровни зрелости согласно CMMI.
24. Опишите сущность стандарта ISO/IEC 17799 и применения модели PDSA к процессам СУИБ/СМЗИ.
25. Назовите основной принцип модели управления ИТ согласно CobiT.

26. Каким правилам стоит следовать при внедрении лучших практик ITIL, CobiT, ISO/IEC 17799.
27. На чем основан подход Microsoft (MSM) к управлению сетевой и информационной инфраструктурой? В чем заключается характерное отличие MSM от ITIL?
28. Что определяет стандарт ГОСТ Р ИСО/МЭК 15408?
29. На какие государственные службы возложены полномочия контроля и надзора в области обеспечения безопасности персональных данных? Каковы функции данных гос. служб в рамках указанных полномочий?
30. Что должно быть обеспечено в ИСПДн в части защиты ПДн?
31. Какие нормативно-методические документы, которые регламентируют вопрос защиты ПДн?
32. Дайте определение категорий персональных данных.
33. Назовите этапы проведения классификации ИСПДн.
34. Какие характеристики ИСПДн используются при классификации ИСПДн?
35. Решение каких задач обеспечивает базовая модель угроз безопасности ПДн?
36. На чем основано выявление частных угроз безопасности ИСПДн?
37. Какие параметры используются при определении актуальности угрозы ИСПДн?
38. Приведите пример технических решений обеспечения безопасности ПДн.
39. Назовите принципы обеспечения ИБ банковских организаций.
40. Перечислите этапы проектирования СМЗИ банковской организации.
41. Приведите примеры требований стандарта PCI DSS.
42. На кого возлагается ликвидация ЧС согласно требованиям российского законодательства о действиях в нештатных ситуациях.
43. Что необходимо иметь на случай возникновения ЧС?
44. Каковы выгоды от составления детального плана обеспечения бесперебойной деятельности предприятия?
45. Перечислите варианты технических решений восстановления деятельности после бедствия.

46. Какие функции должны быть запланированы (учтены в плане) на случай ЧС?
47. Назовите стадии планирования обеспечения бесперебойной деятельности.

**Лист регистрации изменений и дополнений**

| № п/п | № страницы внесения изменений | Дата внесения изменения | Краткое содержание изменений (основание) | Ф.И.О., подпись | «Согласовано» заве-дующий кафедрой, ведущей дисциплину |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |