МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ

ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Фонды оценочных средств по дисциплине

«АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1. Формируемые дисциплиной компетенции

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы:

ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

ОПК.15 Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений на базе ситуационных центров

ОПК.15.3 Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД

2. Планируемые результаты обучения

Коды компетенций	Планируемый результат
ОПК.11.1	Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем
ОПК.11.2	Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации
ОПК.15.3	Знание основных нормативных документов и стандартов, регулирующих защиту информации и аттестацию систем на предмет соответствия требованиям по защите от несанкционированного доступа (НСД);умение проводить оценку состояния информационных технологий и систем, выявляя уязвимости и риски, связанные с НСД, а также определять уровень защищенности объектов;организация и проведение аудита систем обеспечения информационной безопасности, включая анализ архитектуры систем, процессов и процедур, а также оценку эффективности применяемых мер защиты;умение формулировать обоснованные рекомендации по улучшению защиты информационных систем и сооружений на основе проведенного аудита и анализа угроз.

2. Спецификация теста

Тест по дисциплине «Аудит информационных технологий и систем обеспечения информационной безопасности» представляет собой перечень примерных вопросов, предлагаемых студентам с учетом тем и заданий для контрольных мероприятий, предусмотренных по дисциплине.

Тест по дисциплине
«Аудит информационных технологий и систем обеспечения информационной безопасности»

В тесте *может быть несколько правильных ответов.*

Вариант №1

1 Какие есть критерии аудита информационной безопасности
а) Требования законодательства и НМД регуляторов
б) Стандарты в области информационной безопасности
в) Политика информационной безопасности в организации
г) Требования по охране труда

2. Этапы работ по аудиту ИБ
а) Инициирование процедуры аудита;
б) Сбор информации аудита;
в) Анализ данных аудита;
г) Выработка рекомендаций;

3. Какие цели аудита информационной безопасности?
а) Оценка рисков информационной безопасности ;
б) Оценка текущего уровня защищенности в соответствии с критериями аудита информационной безопасности;
в) Поиск и локализация узких мест в системе защиты;
г) Оценка соответствия существующим стандартам в области информационной безопасности и политике безопасности организации;

4. Отличие понятий информационной безопасности и защиты информации
а) Нет разницы в понятиях;
б) Информационная безопасность состояние защищенности информационных активов организации, защита информации деятельность по поддержанию состояния защищенности;
в) Защита информации состояние защищенности информационных активов организации, Информационная безопасность деятельность по поддержанию состояния защищенности.
г) Защита информации противодействие злоумышленникам, Информационная безопасность деятельность по поддержанию состояния защищенности.

5. Какие бывают стандарты, требования и методические документы в области ИБ
а) Приказы регуляторов в области информационной безопасности;
б) ГОСТы
в) Федеральные законы
г) Строительные нормы

6. Для каких информационных систем обязательны требования регуляторов в области информационной безопасности
а) Объекты информатизации обрабатывающие государственную тайну;
б) ИСПДн;
в) ГИС;
г) АСУТП.

7. Требования для обеспечения информационной безопасности для государственных информационных систем закреплены в нормативных документах?
а) ФЗ №149 от 27.07.2006
б) Приказ ФСТЭК России от 11 февраля 2013 г. № 17

в) Приказ ФСТЭК от 18 февраля 2013 г. №21
г) ГОСТ РО 0043-004-2013

8. Какие мероприятия необходимо выполнить для поиска средств негласного съема информации в помещениях

а) Специальное обследование помещения.
б) Специальную проверку технических средств.
в) Специальные лабораторные исследования технических средств.
г) Специальную экспертизу организации на соответствии лицензионным требованиям.

9. Риск нарушения информационной безопасности это

а) производная величины потенциального негативного воздействия и ущерба для активов организации и вероятности реализации угрозы ИБ;
б) вероятность уязвимости актива;
в) ценность актива организации;
г) потери при инциденте ИБ.

10. Что из перечисленного не является целью проведения анализа рисков?

а) Делегирование полномочий
б) Количественная оценка воздействия потенциальных угроз
в) Выявление рисков
г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

11. Что из перечисленного не является задачей руководства в процессе аудита ИБ?

а) Поддержка службы информационной безопасности;
б) Выполнение разработки политики ИБ;
в) Определение и утверждение цели и границ аудита;
г) Делегирование полномочий по принятию рисков ИБ.

12. Какие виды аппаратуры применяется при специальных проверках технических средств?

а) рентгеновские камеры;
б) виброметры;
в) шумомеры;
г) нелинейные локаторы.

13. В каких документах закреплены требования по информационной безопасности персональных данных в организации?

а) Федеральный закон от 27 июля 2006 г. N 152-ФЗ;
б) Постановление правительства РФ от 1 ноября 2012 г. N 1119;
в) Федеральный закон от 27 июля 2006 года № 149-ФЗ;
г) Приказ ФСТЭК от 18 февраля 2013 г. №21.

14. Что представляет собой стандарт ISO/IEC 17799?

а) Стандарт по практическим правилам управления информационной безопасностью;
б) Новая версия BS 17799;
в) Определения для новой серии ISO 27000;
г) Новая версия NIST 800-60.

15. Защита информации это:

а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

16. Стандарты СУИБ по которым возможна сертификация организаций:
а) NIST 800-60;
б) ГОСТ Р ИСО/МЭК 27001;
в) СТО БР ИББС-1.8-2019
г) ГОСТ Р ИСО/МЭК 18045-2013.

17. Может ли стандарт PCI DSS быть критерием при проведении аудита информационной безопасности
а) Может;
б) Не может;
в) Обязан быть для организаций работающих с пластиковыми банковскими картами;
г) Обязан быть для организаций банковской сферы.

18. Для оценки сетевой безопасности организации используются следующие средства тестирования:
а) сниферы
б) сетевые сканеры;
в) средства защиты от несанкционированного доступа;
г) анализаторы трафика.

19. Направления оценки при аудите информационной безопасности организации банковской сферы?
а) текущий уровень ИБ организации;
б) менеджмент ИБ организации;
в) уровень осознания ИБ организации.
г) уровень риска ИБ активов организации

20. Стандарты ЦБ РФ применяемые как критерии информационной безопасности?
а) СТО БР ИББС-1.0-2014
б) СТО БР ИББС-1.1-2007
в) СТО БР ИББС-1.2-2014
г) СТО БР ИББС-1.8-2019

Вариант №2

1. Что проверяется при сертификации СУИБ в организации

а) организационная структура ИБ,
б) политика ИБ,
в) обязанности персонала в области ИБ,
г) ресурсы в области ИБ.

2. Информационная безопасность организации.

а) Состояние защищенности интересов организации в условиях угроз в информационной сфере.
б) Установка средств защиты в АС организации;
в) Процесс оценки и обработки рисков ИБ в организации;
г) Выполнение норм и правил утвержденных руководством.

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации активов?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

5. На каких этапах цикла СУРИБ проходит аудит рисков ИБ?

а) установление контекста управления рисками ИБ;
б) оценка риска ИБ;
в) обработка риска ИБ;
г) коммуникация рисков ИБ.

6. Какие виды аппаратуры применяется при специальных лабораторных исследованиях технических средств на возможность утечки по каналам ПЭМИН?

а) рентгеновские камеры;
б) спектроанализаторы;
в) шумомеры;
г) нелинейные локаторы.

7. Какие стандарты необходимо использовать при создании СЗИ ГИС

а) ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
б) ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».
в) ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».
г) СТО БР ИББС-1.0.

8. Какие мероприятия необходимо выполнить для поиска средств негласного съема информации в технических средствах

а) Специальное обследование помещения.
б) Специальную проверку технических средств.
в) Специальные лабораторные исследования технических средств.
г) Специальную экспертизу организации на соответствии лицензионным требованиям.

9. Остаточный риск ИБ это

а) риск ИБ, остающийся после обработки риска ИБ;
б) риск ИБ перед оценкой рисков;
в) риск обрабатываемый с помощью страхования;
г) риск инцидентов ИБ.

10. В каких документах закреплены требования по информационной безопасности в ИСПДн организации?

а) Приказ ФСТЭК России от 11 февраля 2013 г. № 17;
б) Постановление правительства РФ от 1 ноября 2012 г. N 1119;
в) Федеральный закон от 27 июля 2006 года № 149-ФЗ;
г) Приказ ФСТЭК от 18 февраля 2013 г. №21.

11. Каким стандартом нужно руководствовался при составлении программы аудита ИБ?

а) ГОСТ Р ИСО 19011 - 2012;
б) ISO 17799;
в) СТО БР ИББС-1.0-2014;
г) ISO 27001.

12. Что проверяется при аттестации объектов информатизации

а) распределение обязанностей должностных лиц на объекте,
б) настройки СЗИ на объекте,
в) обязанности руководителя по обеспечению информационной безопасности в организации,
г) политика ИБ в организации.

13. Для тестирования системы реагирования на инциденты в организации используются

а) DLP
б) SIEM
в) ERP
г) IDS

14. Стандарт управления инцидентами ИБ как критерии аудита СУИИБ

а) ISO/IEC 27035:2011
б) ISO/IEC 17799
в) ISO 27001
г) NIST 800-60

15. Какие разделы СТО БР ИББС-1.0-2014 становятся критериями аудита по данному стандарту

а) Модели угроз и нарушителей ИБ организаций БС РФ.
б) Система ИБ организации БС РФ.
в) Система менеджмента ИБ организации БС РФ.
г) Проверка и оценка ИБ организаций БС РФ.

16. Стандарты СУИБ как критерии аудита организации:

а) ISO/IEC 17799;
б) ГОСТ Р ИСО/МЭК 27001-2006;
в) ISO/IEC 9001;
г) ГОСТ Р ИСО/МЭК 18045-2013.

17. Методы проверки соответствия требованиям стандарта PCI DSS

а) внешний аудит, выполняемый экспертной компанией на объекте проверяемой организации;
б) заполнение листа самооценки;
в) автоматизированное сканирование уязвимостей периметра сети;
г) оценка рисков платежным системам.

18. Какие организации имеют право выдавать аттестаты соответствия требованиям безопасности на ОИ, обрабатывающие конфиденциальную информацию

а) лицензиаты ФСБ;
б) лицензиаты ФСТЭК по ТЗКИ;
в) ФСТЭК;
г) органы по аттестации ОИ.

19. Обработка рисков ИБ это:

а) процесс измерения риска ИБ;
б) процесс выбора и реализации мер по изменению риска ИБ ;
в) процесс выбора и осуществления защитных мер, снижающих риски ИБ, или мер по переносу, принятию или уходу от рисков ИБ ;
г) процесс выбора и осуществления мер по модификации (изменению) рисков ИБ.

20. Действующие стандарты ЦБ РФ в области СМИБ в которых описана методика аудита информационной безопасности организации банковской сферы?

а) СТО БР ИББС-1.0-2014
б) СТО БР ИББС-1.0-2007
в) СТО БР ИББС-1.1-2007
г) СТО БР ИББС-1.3-2019

Ключ к тесту

Вариант 1	Вариант 2
1. а,б,в	1 а,б,в
2. а,б,в,г	2 а
3. а,б,в,г	3 в
4. б	4 б
5. а,б,в	5 а,б
6. а,б,в	6 б
7. б	7 а,б
8. а,б	8 б
9. а	9 а
10. б,в,г	10 б,в,г
11. б	11 а
12. а	12 а,б
13. а,б,г	13 б
14. а	14 а
15. г	15 б
16. б	16 а,б
1 7. а, в	17 а,б,в
18. а,б,г	18 б
19. а,б,в	19 в
20. а	20 в