Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 05.09.2026 12:33:11
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"26" февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аудит информационной безопасности»

Направление подготовки
«10.05.03 Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
к.т.н.  /С.А. Кесель/

Ассистент кафедры «Информационная безопасность»  /А.В. Шорников/

Согласовано:
Заведующий кафедрой «Информационная безопасность»,
к.т.н., доцент  /И.В. Калуцкий/

Руководитель образовательной программы
ст. преподаватель кафедры «Информационная безопасность»  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 4
3.1 Виды учебной работы и трудоемкость 4
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
3.4 Тематика семинарских/практических и лабораторных занятий 7
3.5 Тематика курсовых проектов (курсовых работ) 7
4 Учебно-методическое и информационное обеспечение 7
4.1 Нормативные документы и ГОСТы 7
4.2 Основная литература 7
4.3 Дополнительная литература 7
4.4 Электронные образовательные ресурсы 8
4.5 Лицензионное и свободно распространяемое программное обеспечение 8
4.6 Современные профессиональные базы данных и информационные справочные системы 8
5 Материально-техническое обеспечение 8
6 Методические рекомендации 8
6.1 Методические рекомендации для преподавателя по организации обучения 8
6.2 Методические указания для обучающихся по освоению дисциплины 8
7 Фонд оценочных средств 9
7.1 Методы контроля и оценивания результатов обучения 9
7.2 Шкала и критерии оценивания результатов обучения 9
7.3 Оценочные средства 9

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Аудит информационной безопасности» следует отнести:

- изучение студентами видов, практических методов и средств проведения аудита информационной безопасности (ИБ).

К **основным задачам** освоения дисциплины «Аудит информационной безопасности» следует отнести:

- формирование понимания процессов проверки и оценки метрик ИБ, принципов организации процессов аудита и анализа рисков ИБ и подготовки отчетных документов;
- ознакомление с основными стандартами в области аудита ИБ, практическими приемами проведения аудита, методами сбора данных, оценки рисков и анализа защищенности, инструментальными средствами проведения аудита ИБ.

Обучение по дисциплине «Аудит информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ИОПК-10.1. Знает принципы формирования политики информационной безопасности в информационных системах; ИОПК-10.2. Умеет разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. ИОПК-10.3. Владеет методами работы технического специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты
ПК-2. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИПК-2.1. Знает организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем; ИПК-2.2. Умеет участвовать в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; ИПК-2.3. Владеет методиками проверки защищенности объектов информатизации на соответствие нормативных документов.
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. Владеет методами организации и управления деятельность служб защиты информации на предприятии.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части Б1 «Дисциплины (модули)».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы управления информационной безопасностью», «Организационно-правовое обеспечение информационной безопасности», «Аналитика информационной безопасности», «Мониторинг событий и управление инцидентами (SIEM)».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	**7**	**1-18**
	В том числе:			
1.1	Лекции	18	7	1-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	54	7	1-18
2	**Самостоятельная работа**	**72**	**7**	**1-18**
3	**Промежуточная аттестация**		**7**	**19-21**
	Дифференцированный зачет		7	19-21
	Итого	**144**		

3.1.2 Очно-заочная форма обучения

Не предусмотрена.

3.1.3 Заочная форма обучения

Не предусмотрена.

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Аудит информационной безопасности.	**28**	**6**		**4**		**18**
1.1	Тема 1.1. Аудит информационной безопасности. Понятия, определения и методика		2				6
1.2	Тема 1.2. Анализ защищенности. Пентестирование.		2				6
1.3	Тема 1.3. Аудит соответствия требованиям Российского законодательства в области информационной безопасности		2		4		6
2	Раздел 2. Аудит соответствия PCI DSS.	**72**	**6**		**42**		**24**
2.1	Тема 2.1. Аудит соответствия PCI DSS. Обзор стандарта PCI DSS.		2		18		6
2.2	Тема 2.2. Аудит соответствия PCI DSS. Внедрение стандарта PCI DSS.		2		24		6
2.3	Тема 2.3. Аудит соответствия PCI DSS. Область применимости требований PCI DSS		1				6
2.4	Тема 2.4. Аудит соответствия PCI DSS. Сужение области применимости стандарта PCI DSS		1				6
3	Раздел 3. Аудит соответствия СТО БР.	**44**	**6**		**8**		**30**
3.1	Тема 3.1. Аудит соответствия СТО БР. Общие положения.		1		8		6
3.2	Тема 3.2. Аудит соответствия СТО БР		1				6
3.3	Тема 3.3. Аудит соответствия СТО БР. Методики оценки соответствия.		2				6
3.4	Тема 3.4. Аудит соответствия СТО БР. Методика оценки рисков нарушения информационной безопасности		1				6
3.5	Тема 3.5. Аудит соответствия СТО БР. Самооценка соответствия информационной безопасности		1				6
Итого		**144**	**18**		**54**		**72**

3.2.2 Очно-заочная форма обучения

Не предусмотрена

3.2.3 Заочная форма обучения

Не предусмотрена

3.3 Содержание дисциплины

Раздел 1. Аудит информационной безопасности.

Тема 1.1. Аудит информационной безопасности. Понятия, определения и методика. Предмет, содержание и цели курса, формы отчетности, основная и дополнительная литература, ГОСТ Р ИСО/МЭК 19011-2021, ГОСТ Р ИСО/МЭК 27001-2021, планирование аудита, границы аудита.

Тема 1.2. Анализ защищенности. Пентестирование. Этичный хакинг, методология оценки рисков, применение метрик CVSS v3.1, EPSS и списков KEV, инструментальное сканирование, аудит в формате «черного ящика», формирование реестра уязвимостей.

Тема 1.3. Аудит соответствия требованиям Российского законодательства в области информационной безопасности. Аттестация объектов информатизации, требования ФСТЭК и ФСБ по защите ГИС и ИСПДн, средства защиты информации, разработка акта классификации, технического паспорта и аттестата соответствия.

Раздел 2. Аудит соответствия PCI DSS.

Тема 2.1. Аудит соответствия PCI DSS. Обзор стандарта PCI DSS. Требования международных платежных систем, безопасность данных держателей карт, уровни комплаенса, 12 основных требований стандарта.

Тема 2.2. Аудит соответствия PCI DSS. Внедрение стандарта PCI DSS. Процесс QSA-аудита, заполнение листов самооценки SAQ, формирование отчета о соответствии (ROC), использование компенсирующих мер.

Тема 2.3. Аудит соответствия PCI DSS. Область применимости требований PCI DSS. Определение среды данных владельцев карт (CDE), инвентаризация потоков данных, идентификация системных компонентов.

Тема 2.4. Аудит соответствия PCI DSS. Сужение области применимости стандарта PCI DSS. Сегментация сети, использование технологий токенизации и шифрования, аутсорсинг функций ИБ.

Раздел 3. Аудит соответствия СТО БР.

Тема 3.1. Аудит соответствия СТО БР. Общие положения. Нормативная база ЦБ РФ, цели и область распространения стандартов Банка России, требования к обеспечению информационной безопасности в организациях банковской системы.

Тема 3.2. Аудит соответствия СТО БР. Процедура внешней проверки, взаимодействие финансовой организации с регулятором и аудиторскими компаниями.

Тема 3.3. Аудит соответствия СТО БР. Методики оценки соответствия. Оценка групповых показателей, расчет итогового балла соответствия ИБ по установленным метрикам.

Тема 3.4. Аудит соответствия СТО БР. Методика оценки рисков нарушения информационной безопасности. Матрица рисков, триада конфиденциальности, целостности и доступности, классификация активов, метрики ROI и SLA.

Тема 3.5. Аудит соответствия СТО БР. Самооценка соответствия информационной безопасности. Внутренний аудит, чек-листы самопроверки, модель зрелости процессов CMMI, непрерывный мониторинг и улучшение системы защиты.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

Раздел 1. Аудит информационной безопасности.

Лабораторная работа №1. Аудит соответствия кредитно-финансовых организаций РФ требованиям законодательства РФ в области ИБ

Раздел 2. Аудит соответствия PCI DSS

Лабораторная работа №2. Аудит соответствия кредитно-финансовых организаций РФ требованиям Федерального закона от 27.07.2006 №152-ФЗ (О персональных данных)

Лабораторная работа №3. Получение лицензии ФСБ на криптографию для банковской организации

Раздел 3. Аудит соответствия СТО БР.

Лабораторная работа №4. Аудит соответствия кредитно-финансовых организаций РФ требованиям российского законодательства в области информационной безопасности СТО БР ИББС-1.0-2014 (Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения)

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрены учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. ГОСТ Р ИСО/МЭК 19011-2021. Руководящие указания по аудиту систем менеджмента. — Москва : ФГБУ «РСТ», 2021. — 44 с.
2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Москва : ФГБУ «РСТ», 2021. — 32 с.
3. ГОСТ Р 57580.2-2021. Безопасность финансовых (банковских) операций. Контроль защиты информации. Методика оценки соответствия. — Москва : ФГБУ «РСТ», 2021. — 56 с.
4. О персональных данных : Федеральный закон от 27 июля 2006 года № 152-ФЗ. — Текст : электронный // Доступ из справочно-правовой системы «КонсультантПлюс».
5. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 года № 187-ФЗ. — Текст : электронный // Доступ из справочно-правовой системы «КонсультантПлюс».
6. Об утверждении Требований о защите информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 года № 17. — Текст : электронный // Доступ из справочно-правовой системы «КонсультантПлюс».
7. Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации : положение Банка России от 17 апреля 2019 года № 683-П. — Текст : электронный // Доступ из справочно-правовой системы «КонсультантПлюс».

8. PCI DSS Version 4.0.1. Payment Card Industry Data Security Standard. Requirements and Testing Procedures. — Text : electronic // PCI Security Standards Council : official site. — 2024. — URL: https://www.pcisecuritystandards.org (date of access: 14.05.2026).
9. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. — Москва : Стандартинформ, 2017. — 60 с.

4.2 Основная литература

1. Скаржевская, Е. О. Аудит информационной безопасности : учебное пособие для вузов / Е. О. Скаржевская, А. А. Сковпень. — Москва : Издательство Юрайт, 2024. — 134 с.
2. Ермакова, А. С. Аудит информационной безопасности : учебник / А. С. Ермакова. — Санкт-Петербург : Лань, 2022. — 216 с.
3. Овчинников, В. В. Информационная безопасность: защита и аудит : учебник / В. В. Овчинников. — Москва : КноРус, 2023. — 288 с.

4.3 Дополнительная литература

1. Common Vulnerability Scoring System v3.1 : Specification Document. — Text : electronic // FIRST — Forum of Incident Response and Security Teams : official site. — 2023. — URL: https://www.first.org/cvss/v3.1/specification-document.
2. Known Exploited Vulnerabilities (KEV) Catalog. — Text : electronic // Cybersecurity & Infrastructure Security Agency (CISA) : official site. — 2026. — URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
3. Information Supplement: Guidance for PCI DSS Scope Segmentation and Tokenization. — Version 2.0. — Text : electronic // PCI Security Standards Council : official site. — 2021. — URL: https://www.pcisecuritystandards.org.
4. Уокер, М. CEH. Сертифицированный этичный хакер. Экзаменационное руководство / М. Уокер. — 5-е изд. — Москва : Диалектика-Вильямс, 2022. — 800 с.
5. Абрамов, В. С. Управление рисками и аудит ИБ в банковских системах : монография / В. С. Абрамов. — Москва : Университетская книга, 2021. — 192 с.

4.4 Электронные образовательные ресурсы

Электронный курс «Аудит информационной безопасности» [Электронный ресурс] // Электронная информационно-образовательная среда Московского политеха / URL: https://online.mospolytech.ru/course/view.php?id=2014.

4.5 Лицензионное и свободно распространяемое программное обеспечение

В рамках освоения дисциплины, дополнительное программное обеспечение не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. КонсультантПлюс: справочная правовая система [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.consultant.ru/.
2. Гарант: информационно-правовой портал [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.garant.ru/
3. eLIBRARY.RU: научная электронная библиотека [Электронный ресурс]. – Режим доступа: свободный. URL: https://elibrary.ru/.
4. Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/ – Режим доступа: для авториз. пользователей.
5. Образовательная платформа «Юрайт» : [сайт]. – URL: https://urait.ru/ – Режим доступа: для авториз. пользователей.
6. Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprsmart.ru/ – Режим доступа: для авториз. пользователей.

5 Материально-техническое обеспечение

Лабораторные работы и самостоятельная работа студентов должны проводиться в специализированной аудитории, оснащенной современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащено современным компьютером с подключенным к нему проектором на настенный экран, или иным аналогичным по функциональному назначению оборудованием.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов является самостоятельная работа, а также посещение аудиторных занятий.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях. Оценивание результатов обучения по дисциплине осуществляется на основе балльно-рейтинговой системы (далее – БРС). Максимальный совокупный балл за академический период составляет 100.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь в проверке гипотез и задумок. Однако выполнять задания и оформлять отчетные материалы студент должен самостоятельно. Делиться отчетными материалами или создавать их совместно запрещено.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы обучающиеся регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения. Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей. По усмотрению преподавателя студенту могут начисляться дополнительные баллы за активную работу в семестре, участие в научных мероприятиях, нестандартные решения задач и другие достижения. Такие баллы суммируются с основной оценкой, но итоговый результат не может превышать 100 баллов.

После сдачи (загрузки в СДО) лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет содержание отчета, таблиц, исходного кода и других отчетных материалов, а также выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по предоставленным отчетным материалам, а также теоретическим вопросам, приведенных после текста задания лабораторной работы (при их наличии). Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она не оценивается, либо оценка будет снижена на усмотрение преподавателя.

За каждую лабораторную работу устанавливается максимально возможное количество рейтинговых баллов в соответствии с пунктом 7.2. При несвоевременной сдаче работы (позднее срока, установленного в календарно-тематическом плане) количество начисляемых баллов может быть снижено:

- при сдаче работы с опозданием до 3 календарных дней – максимально возможное количество баллов снижается на 10% (оценка за лабораторную работу выставляется с коэффициентом – 0.9);

- при сдаче работы с опозданием от 4 до 7 календарных дней – максимально возможное количество баллов снижается на 25% (оценка за лабораторную работу выставляется с коэффициентом – 0.75);
- при сдаче работы с опозданием свыше 7 календарных дней – начисляется не более 50% от максимально возможного количества баллов за задание (оценка за лабораторную работу выставляется с коэффициентом – 0.5).

В случае наличия уважительных причин для несвоевременной сдачи работы, студент должен обратиться к преподавателю. При возможности, студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей лабораторной работы или иного полученного задания.

Работа должна быть выполнена студентом самостоятельно: в отчетных материалах должны содержаться результаты работы только за его авторством, по отчетным материалам можно проследить как велась работа, студент может объяснить ход выполнения работы, если же обозначенное выше не соблюдается, то такая работа не считается сданной и не оценивается.

Рубежные контроли выполняются в аудитории индивидуально по варианту задания, выданному преподавателем в назначенные дни. При отсутствии студента в день написания контрольной работы ему дается еще один шанс ее написать на другом занятии в семестре (в том числе и в рамках консультаций преподавателя), но обязательно очно.

7.2 Шкала и критерии оценивания результатов обучения

За посещение аудиторных занятий начисляется до 9 баллов (по 0,5 балла за каждое занятие при условии регулярного посещения). При пропуске занятий количество баллов уменьшается пропорционально количеству пропусков.

За выполнение лабораторных работ начисляется до 47 баллов, более конкретное распределение баллов за лабораторные работы представлено ниже:

Лабораторная работа №1, №2 – до 10 баллов.

Лабораторная работа №3 – до 15 баллов.

Лабораторная работа №4 – до 12 баллов.

За прохождение рубежного контроля начисляется до 8 баллов. За первый и второй рубежный контроль можно получить до 2 баллов, за третий рубежный контроль можно получить до 3 баллов.

Итого, по результатам текущего контроля, не считая дополнительных баллов, студент может получить до 64 баллов.

В свою очередь, по результатам промежуточной аттестации студент может получить до 36 баллов. Студенты, получившие оценку «неудовлетворительно» в ходе промежуточной аттестации, сохраняют ранее накопленную оценку за текущий контроль.

Итоговая оценка по дисциплине (модулю) определяется по следующим критериям:

- «неудовлетворительно» (2) – 0-54 баллов;
- «удовлетворительно» (3) – 55-69 баллов;
- «хорошо» (4) – 70-84 баллов;
- «отлично» (5) – 85-100 баллов.

7.3 Оценочные средства

7.3.1 Текущий контроль

Оценочными средствами текущего контроля являются лабораторные работы, выложенные в курсе СДО по данной дисциплине (модулю), а также прохождение рубежных контролей.

7.3.2 Промежуточная аттестация

Формой оценки знаний в рамках промежуточной аттестации является: ***дифференцированный зачет***.

В ходе промежуточной аттестации студенту выдается билет, содержащий 3 вопроса. За ответ на каждый вопрос студент может получить до 12 баллов. Билет формируется из перечня вопросов, расположенного ниже:

1. Аудит ИБ. Концепция IA*4
2. Оценочные стандарты и спецификации ИБ.
3. Состав, основные стандарты и спецификации.
4. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?
5. Что такое персональные данные в соответствии с ФЗ-152?
6. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?
7. Раскройте понятие "конфиденциальный документ"
8. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.
9. В каком случае фотографию можно отнести к биометрическим персональным данным?
10. Может ли являться оператором персональных данных физическое лицо?
11. Какие действия можно производить с персональными данными?
12. Перечислите классификационные группы персональных данных по признаку свободы оборота.
13. Кто является основным ответственным за определение уровня классификации информации?
14. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
15. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
16. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
17. Основной документ, на основе которого проводится политика информационной безопасности?
18. Коммерческая тайна это….
19. Государственная тайна это…
20. Банковская тайна это….
21. Профессиональная тайна…
22. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

23. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
24. Стандарт «Общие Критерии». Концепция, основные понятия и определения.
25. Стандарт «Общие Критерии». Оценочные уровни доверия (ОУД)
26. СТО БР ИББС Структура, концепция, основные понятия и определения.
27. СТО БР ИББС Проведение аудита соответствия кредитно-финансовой организации требованиям СТО БР ИББС.
28. PCI DSS Структура, концепция, основные понятия и определения.
29. PCI DSS Проведение аудита соответствия требованиям PCI DSS
30. PCI DSS Проведение самооценки соответствия требованиям PCI DSS
31. PCI DSS Основные требования (12 требований)

Пример экзаменационного билета

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_
по дисциплине

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
10.05.03 Информационная безопасность автоматизированных систем

ВОПРОСЫ:

1. Коммерческая тайна это...
2. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
3. Кто является основным ответственным за определение уровня классификации информации?

Утверждено: _____ / _____ / «__» _____ 20__г.