Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Кафедра информационной безопасности
Факультета информационных технологий и анализа больших данных**

УТВЕРЖДАЮ

Проректор по учебной и
методической работе

_____Е.А. Каменева

«18» ноября 2024 г.

Марков А.С., Капинос С.П.

Аудит кибербезопасности цифрового предприятия

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
10.04.01 «Информационная безопасность»
направленность программы магистратуры:
«Управление информационной безопасностью в кредитно-финансовой сфере»

*Рекомендовано Ученым советом Факультета
информационных технологий и анализа больших данных
(протокол от «30» октября 2024 г. № 48)*

*Одобрено на заседании Кафедры информационной безопасности
(протокол от «05» сентября 2024 г. № 7)*

Москва 2024

СОДЕРЖАНИЕ

1. Наименование дисциплины

Аудит кибербезопасности цифрового предприятия.

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Таблица 1

Код компе-тенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
УК-1	Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий	1. Использует методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности.	**Знать** Методы анализа информации и синтеза проблемных ситуаций **Уметь** проводить анализ информации и синтез формализованных моделей процессов и явлений в профессиональной деятельности
		2. Демонстрирует способы осмысления и критического анализа проблемных ситуаций.	**Знать** способы критического анализа проблемных ситуаций **Уметь** проводить критический анализ проблемных ситуаций
		3. Предлагает нестандартное решение проблем, новые оригинальные проекты, вырабатывает стратегию действий на основе системного подхода.	**Знать** стратегии действий на основе системного анализа **Уметь** применять нестандартное решение проблем и вырабатывать стратегию действий на основе системного подхода

ПКН-1	Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов	1. Использует отечественные и зарубежные стандарты в области обеспечения информационной безопасности.	**Знать** отечественные и зарубежные стандарты в области обеспечения информационной безопасности. **Уметь** выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов на основе отечественных и зарубежных стандартов в области обеспечения информационной безопасности.
		2. Разрабатывает требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности.	**Знать** требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности. **Уметь** разрабатывать требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности на основе проведенного анализа состояния существующих требований
		3. Демонстрирует навыки разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	**Знать** стратегии решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности. **Уметь** разрабатывать стратегии решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.
ПКН-3	Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	1. Применяет нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного	**Знать** нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации. **Уметь** применять нормативные правовые акты, нормативные и методические документы,

		доступа, проектирования и сертификации средств защиты информации.	национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации.
		2. Использует необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Знать** существующие нормативные правовые акты и актуализированные нормативные акты **Уметь** использовать нормативные правовые акты по обеспечению информационной безопасности
		3. Составляет организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Знать** перечень организационно-распорядительных документов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации. **Уметь** разрабатывать проекты организационно-распорядительных документов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации.
ПК-2	Способность определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы	1 Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем кредитно-финансовой сферы	**Знать** комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем кредитно-финансовой сферы **Уметь** определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы

		2 Проводит оценку возможностей внешних и внутренних нарушителей	**Знать** возможности внешних и внутренних нарушителей **Уметь** проводить оценку возможностей внешних и внутренних нарушителей
		3 Разрабатывает модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы	**Знать** модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы **Уметь** разрабатывать модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы
ПК-4	Способность моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	1 Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы	**Знать** аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы **Уметь** разрабатывать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы
		2 Исследует аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы	**Знать** аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы **Уметь** проводить исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы
		3 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы	**Знать** системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы **Уметь** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы

3. Место дисциплины в структуре образовательной программы

Дисциплина «Аудит кибербезопасности цифрового предприятия» относится к модулю дисциплин по выбору, углубляющих освоение направленности программы магистратуры.

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 2

Вид учебной работы по дисциплине	**Всего (в з.е и часах)**	**Модуль 6 (в часах)**
Общая трудоемкость дисциплины	4 з.е./144 ч.	144
Контактная работа-Аудиторные занятия	60	60
Лекции	20	20
Семинары, практические занятия	40	40
Самостоятельная работа	84	84
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Раздел 1. Основы киберпространства и кибербезопасности

Введение в кибербезопасность и киберпространство. Информационная безопасность и риски. Структура информационного пространства в Российской Федерации. Протоколы и платформы. Архитектура сетевой безопасности и управление процессом обеспечения безопасности. Архитектура автоматизированных информационных систем.

Раздел 2. Векторы риска

Система поставок/поставщики. Удалённые сетевые атаки. Вторжение в систему лиц, обладающих правом доступа. Риски, связанные с мобильностью, утечкой данных.

Раздел 3. Международные организации по кибербезопасности, принципы и стандарты

Международные организации по кибербезопасности. Международные и

национальные стандарты по кибербезопасности. Национальные механизмы кибербезопасности. Кибербезопасность в российском и международном законодательстве.

5.2. Учебно-тематический план

Таблица 2

п/п	Наименование тем (разделов) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа*- Аудиторная работа			Самостоятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия		
1.	Раздел 1. Основы киберпространства и кибербезопасности	**52**	24	8	16	28	доклады, презентации дискуссии
2.	Раздел 2. Векторы риска	**44**	16	6	10	28	доклады презентации дискуссии
3.	Раздел 3. Международные организации по кибербезопасности, принципы и стандарты	**48**	20	6	14	28	доклады презентации дискуссии.
	В целом по дисциплине	**144**	**60**	**20**	**40**	**84**	Согласно учебному плану: Контрольная работа
	Итого в %		42	33	67	58	

*Объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

5.3. Содержание семинаров, практических занятий

Таблица 3

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
1. Основы киберпространства и кибербезопасности	1.Введение в кибербезопасность и киберпространство. 2.Информационная безопасность и риски. 3.Структура информационного пространства в Российской Федерации. 4.Протоколы и платформы. 5.Архитектура сетевой безопасности и управление процессом обеспечения безопасности. Рекомендуемые источники: 8.1, 8.3, 8.5, 9.1, 9.2, 9.10, 9.11, 9.12	Дискуссии Презентации Разбор ситуаций
2. Векторы риска	1.Система поставок/поставщики. 2.Удалённые сетевые атаки. 3.Вторжение в систему лиц, обладающих правом доступа. 4.Риски, связанные с мобильностью, утечкой данных. Рекомендуемые источники: 8.1,8.2, 9.3,9.4, 9.9, 9.10, 9.11, 9.12	Дискуссии Презентации Разбор ситуаций
3.Международные организации по кибербезопасности, принципы и стандарты	1.Международные организации по кибербезопасности. 2.Международные стандарты по кибербезопасности. 3.Национальные механизмы кибербезопасности. 4.Кибербезопасность в российском и международном законодательстве. Рекомендуемые источники: 8.1,8.2,8.3, 8.4, 9.1, 9.2, 9.3,9.4, 9.11, 9.12	Дискуссии Презентации Разбор ситуаций

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

6.1 Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы

1. Основы киберпространства и кибербезопасности	1. Концепции стратегии кибербезопасности РФ; . Стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности». 3. Основные документы по вопросам информационной безопасности РФ. 4. Общая структура и конкретная топология Интернета в Российской Федерации 5. Стандарты сетевых и информационных технологий 6. Основы анализа угроз, рисков и уязвимостей	- работа с учебной, научной и справочной литературой; - подготовка докладов по теме; - подготовка презентаций по теме.
2.Векторы риска	1. Управление цепями *поставок* (англ. supply chain management, SCM) 2. Основные виды сетевых атак 3. Архитектура подсистемы защиты ОС 4. Корпоративная мобильность (Bring Your Own Device – BYOD)	- работа с учебной, научной и справочной литературой; - подготовка докладов по теме; - подготовка презентаций по теме
3.Международные организации по кибербезопасности, принципы и стандарты	1. Кибербезопасность и международное право 2. Основные международные стандарты по информационной безопасности 3. Основные российские стандарты и документы по информационной безопасности	- работа с учебной, научной и справочной литературой; - подготовка докладов по теме; - подготовка презентаций по теме

6.2 Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерный перечень вопросов к контрольной работе

1. Основные различия подходов к кибербезопасности в различных национальных и культурных контекстах.
2. Проблемы в области информационно-коммуникационных технологий.
3. Основные стандарты и протоколы в проектировании Интернета.
4. Основные атаки в информационной среде. Примеры алгоритмов.
5. Анализ уязвимости к угрозам в рамках управления информационной безопасностью.
6. Организации Российской Федерации, ответственные за формулирование государственной политики, практических мер и процедур в сфере обеспечения информационной безопасности.
7. Структура мобильных сетей Интернета.
8. Концепции виртуализации сетевых устройств и определяемых программным обеспечением сетей.
9. Основные элементы управления промышленными объектами на основе SCADA.
10. Международные и российские стандарты и руководящие указания для проведения оценок угроз и рисков, подготовки концепций сетевой безопасности для предприятий и организаций, создания архитектуры элементов безопасности сетей.
11. Роль организации структуры в контексте безопасности системы поставок.
12. Основные сценарии нападения на основе удаленного доступа.
13. Описать сценарий нападения со стороны клиента - подделка межсайтовых запросов и использование веб-браузеров в своих целях.
14. Угрозы для организации, которые могут исходить от ее сотрудников.
15. Аспекты политики мобильности и использования личных устройств на работе в контексте архитектуры безопасности предприятия.
16. Элементы национальной политики информационной безопасности.
17. Основные ключевые вызовы и источники стратегий в международном киберзаконодательстве.

Примерный перечень тем докладов, презентаций:

1. Концепции виртуализации сетевых устройств и определяемых программным обеспечением сетей.

2. Организации Российской Федерации, ответственные за формулирование государственной политики, практических мер и процедур в сфере обеспечения информационной безопасности.

3. Роль организации структуры в контексте безопасности системы поставок.

4. Элементы национальной политики информационной безопасности.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, знаний и умений

Таблица 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
УК-1 Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий	1. Использует методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности.	**Знать** Методы анализа информации и синтеза проблемных ситуаций **Уметь** проводить анализ информации и синтез формализованных моделей	**Задание 1** Разработать алгоритм проведения анализа информации

		процессов и явлений в профессиональной деятельности	
	2Демонстрирует способы осмысления и критического анализа проблемных ситуаций.	**Знать** способы критического анализа проблемных ситуаций **Уметь** проводить критический анализ проблемных ситуаций	**Задание 1** Провести критический анализ проблемных ситуаций на примере конкретной организации
	3. Предлагает нестандартное решение проблем, новые оригинальные проекты, вырабатывает стратегию действий на основе системного подхода.	**Знать** стратегии действий на основе системного анализа **Уметь** применять нестандартное решение проблем и вырабатывать стратегию действий на основе системного подхода	**Задание 1** Предложите нестандартное решение проблемы и выработайте стратегию действий на основе системного подхода и ранее проведенного анализа
ПКН-1 Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов	1. Использует отечественные и зарубежные стандарты в области обеспечения информационной безопасности.	**Знать** отечественные и зарубежные стандарты в области обеспечения информационной безопасности. **Уметь** выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов на основе отечественных и зарубежных стандартов в области обеспечения информационной безопасности.	**Задание 1** Используя отечественные и зарубежные стандарты в области обеспечения информационной безопасности выявите угрозы и оцените уязвимости на примере конкретной организации
	2. Разрабатывает требования к системе обеспечения	**Знать** требования к системе обеспечения	**Задание 1** Для конкретной организации

	информационной безопасности и критерии оценки ее эффективности.	информационной безопасности и критерии оценки ее эффективности. **Уметь** разрабатывать требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности на основе проведенного анализа состояния существующих требований	разработайте требования к системе обеспечения информационной безопасности
	3. Демонстрирует навыки разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	**Знать** стратегии решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности. **Уметь** разрабатывать стратегии решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	**Задание 1** Разработайте стратегии решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.
ПКН-3 Способность разрабатывать проекты организационно-	1. Применяет нормативные правовые акты, нормативные и	**Знать** нормативные правовые акты,	**Задание 1** Провести анализ существующих в

распорядительных документов по обеспечению информационной безопасности	методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации.	нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации. **Уметь** применять нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации.	организации нормативных и правовых актов на предмет актуальности
	2. Использует необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	**Знать** существующие нормативные правовые акты и актуализированные нормативные акты **Уметь** использовать нормативные правовые акты по обеспечению информационно й безопасности	**Задание 1** На основе ранее проведенного анализа составить график актуализации и разработки локальных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации.
	3. Составляет организационно-распорядительные документы, нормативные и методические документы,	**Знать** перечень организационно-распорядительных документов, нормативных и методических	**Задание 1** В соответствии с вариантом задания разработать организационно-распорядительные документы,

	регламентирующие деятельность по защите информации в организации.	документов, регламентирующих деятельность по защите информации в организации. **Уметь** разрабатывать проекты организационно-распорядительных документов, нормативных и методических документов, регламентирующих их деятельность по защите информации в организации.	нормативные и методические документы, регламентирующие деятельность по защите информации в организации
ПК-2 Способность определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы	1 Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем кредитно-финансовой сферы	**Знать** комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем кредитно-финансовой сферы **Уметь** определять угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы	**Задание 1** Определить угрозы безопасности информации, обрабатываемой автоматизированной системой кредитно-финансовой сферы конкретной организации
	2 Проводит оценку возможностей внешних и внутренних нарушителей	**Знать** возможности внешних и внутренних нарушителей **Уметь** проводить оценку	**Задание 1** Провести оценку возможностей внешних и внутренних нарушителей

		возможностей внешних и внутренних нарушителей	
	3 Разрабатывает модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы	**Знать** модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы **Уметь** разрабатывать модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы	**Задание 1** Разработать модели угроз безопасности информации автоматизированной системы кредитно-финансовой сферы
ПК-4 Способность моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	1 Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы	**Знать** аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы **Уметь** разрабатывать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы	**Задание 1** Разработать аналитические модели автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы
	2 Исследует аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных	**Знать** аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных	**Задание 1** На примере конкретной организации провести исследование аналитических и компьютерных

	систем кредитно-финансовой сферы	систем кредитно-финансовой сферы **Уметь** проводить исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы	моделей автоматизированных систем и подсистем безопасности автоматизированных систем кредитно-финансовой сферы
	3 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы	**Знать** системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы **Уметь** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы	**Задание 1** Разработать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем кредитно-финансовой сферы

Перечень вопросов для подготовки к зачету

1. Дайте характеристику важности информационно-коммуникационных технологий и того, как они изменяют структуру современных обществ.

2. Основные различия подходов к кибербезопасности в различных национальных и культурных контекстах.

3. Основные ключевые проблемы в области информационно-коммуникационных технологий.

4. Дайте характеристику положительного и отрицательного воздействия

киберпространства на общество.

5. Основные аспекты информированности об угрозах и рисках для эффективного и безопасного функционирования киберпространства.

6. Основы управление Интернетом, его функционирование и поддержание посредством сети государственных, частных и некоммерческих организаций.

7. Роли стандартов и протоколов в проектировании Интернета.

8. Основные военно-политические требования, связанные с киберпространством и управлением Интернетом.

9. Основные стандарты классификации безопасности в сфере информации, а также информационных и электронных систем.

10. Понятие угрозы безопасности информации. Взаимосвязь угроз безопасности информации с источниками, уязвимостью и рисками

11. Основные угрозы информационной безопасности для объекта информатизации предприятий кредитно-финансовой сферы

12. Объективные и субъективные источники угроз безопасности информации на объекте информатизации предприятий кредитно-финансовой сферы.

13. Основные этапы проведения анализа угроз и рисков.

14. Примеры алгоритмов атак в информационной среде.

15. Определения понятий данные, знания, информация, информационная безопасность, алгоритм атаки в информационной среде.

16. Объяснить опасность снижения уязвимости информации и информационных систем, а также значение конфиденциальности, целостности, доступности, подлинности и неотказуемости информации для обеспечения безопасности информационных систем.

17. Объяснить роль анализа уязвимости к угрозам в рамках управления информационной безопасностью.

18. Основные организации Российской Федерации, ответственные за формулирование государственной политики, практических мер и процедур в сфере обеспечения информационной безопасности.

19. Объяснять значение номеров ASN для обеспечения взаимодействия

различных частей Интернета во всем мире, а также объяснять функции Администрации адресного пространства Интернет (IANA),

20. Раскрыть основы взаимоотношения между Интернет-провайдерами первого уровня, Интернет-провайдерами нижестоящих уровней, а также локальными сетями персональных компьютеров конечных пользователей,

21. Объяснить роль полномочных DNS-серверов в обеспечении взаимодействия компонентов Интернета в глобальном масштабе, а также анализировать роль Корпорации по управлению доменными именами и IP- адресами (ICANN).

22. Раскрыть топологию и географию национального киберпространства, включая роль национальных регистраторов и государственных органов, курирующих Интернет-провайдеров.

23. Структура мобильных сетей Интернета и управлении ими.

24. Давать характеристику таких общих сетевых устройств, как концентраторов (хабов), коммутаторов, маршрутизаторов, шлюзов и серверов приложений, описать способы реализации ими уровней протоколов, а также их функцию в сети.

25. Основные концепции виртуализации сетевых устройств и определяемых программным обеспечением сетей, воздействие этих концепций на архитектуру сетей и их связь со средой «облачных вычислений».

26. Описать базовые элементы управления промышленными объектами на основе SCADA.

27. Определять и описывать общие протоколы сетевой безопасности, их взаимодействие с архитектурой сетей, основанной на протоколах различных уровней, и указать, какие конкретные уязвимые места в сети каждый из протоколов призван устранять.

28. Основные международные и российские стандарты и руководящие указания для проведения оценок угроз и рисков.

29. Основные международные и российские стандарты и руководящие указания для подготовки концепций сетевой безопасности для предприятий и

организаций.

30. Основные международные и российские стандарты и руководящие указания для создания архитектуры элементов безопасности сетей.

31. Провести анализ связи этапа определения важных объектов в ходе оценки угроз и рисков и разработки концепции сетевой безопасности предприятия.

32. Раскрыть основные параметры и сферу действия системы обеспечения секретности документов и информации в России.

33. Описать взаимосвязь проверок благонадежности сотрудников и программ допуска к тайне.

34. Дать пояснения значительности и возможным воздействиям на основе используемой цепи поставок, удаленного, внутреннего доступа, нацеленное на уязвимости в киберпространстве и факторы, связанные с упрощением повышенной мобильности.

35. Выявить основные типы компромиссов между безопасностью и частной жизнью, связанные с повышенной мобильностью и другими векторами риска, установленными в данной тематической области.

36. Раскрыть основные вызовы, касающиеся полного производственного цикла.

37. Объяснить роль организации структуры в контексте безопасности системы поставок.

38. Дать пояснения роли и требованиям сформулированных правил и практики в отношении управления риском в сфере системы поставок.

39. Описать сценарий нападения на основе удаленного доступа, выявить составные части такого нападения.

40. Объяснить, как в рамках нападения со стороны сервера получается информация на этапе сбора данных с применением методов, таких как анализ уязвимостей сети и анализа граничных значений.

41. Объяснить, почему инструменты для анализа уязвимости сети имеют ценность, как для нападающего, так и для защитника.

42. Описать как укрепление безопасности на сетевом периметре и

усовершенствование безопасности на сервере привели к разработке и распространению методов нападения со стороны клиента.

43. Описать сценарий нападения со стороны клиента - межсайтовый скриптинг (внедрение выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу).

44. Описать сценарий нападения со стороны клиента - подделка межсайтовых запросов и использование веб-браузеров в своих целях.

45. Объяснить отношения между нападениями со стороны клиента и методами действий на основе обмана, такими как нападения типа «фишинг» (phishing) и нападения на предприятие или отрасль, когда заражается сайт, часто посещаемый сотрудниками данного предприятия.

46. Описать основные угроз организации, которые могут исходить от ее сотрудников.

47. Описать нападения на основе локального доступа и выявить составные части такого нападения.

48. Описать основные методы, применяемые нападающими для злоупотребления своими текущими привилегиями и повышения их уровня.

49. Объяснить применение принципов наименьшего уровня привилегий и служебных обязанностей, а также разработки политики безопасности на их основе.

50. Нормативно-методические документы, регламентирующие порядок проведения аттестации объектов информатизации. Состав организационной структуры системы аттестации объектов информатизации предприятий кредитно-финансовой сферы.

51. Порядок проведения аттестации и контроля объектов информатизации требованиям безопасности информации. Организация документооборота органа по аттестации объекта информатизации предприятий кредитно-финансовой сферы.

52. Основные требования, предъявляемые к политике информационной безопасности. Основные свойства, принципы и жизненный цикл политики информационной безопасности.

53. Провести анализ положительных и отрицательных аспектов в отношении

компромисса между политикой безопасности и пользованием соцсетями на работе с точки зрения работника и работодателя.

54. Основные аспекты политики мобильности и использования личных устройств на работе в контексте архитектуры безопасности предприятия, а также определить компромисс между безопасностью и пользовательскими правами.

55. Провести анализ политики в отношении использования «облаков» при хранении и обработке информации в государственном и коммерческом контекстах.

56. Описать основные российские организации, отвечающие за кибербезопасность.

57. Определить и понять роль и требования национальных и международных ведомств по стандартам.

58. Пояснить важность отношений между кибербезопасностью, спецслужбами и военными институтами.

59. Основная роль ключевых международных организаций, играющих лидирующую роль в кибербезопасности.

60. Сформулировать различные проблемы, касающиеся правительств и их взаимодействия с международными организациями по вопросам кибербезопасности.

61. Основные крупнейшие международные организации, их руководящие принципы и их роль в информировании, а также поддержке национальной кибербезопасности.

62. Основные международные организации по развитию стандартов (напр., ISO, NIST).

63. Определить ключевые элементы национальной политики информационной безопасности.

64. Основные источники передового опыта в организации национальной кибербезопасности.

65. Основные ключевые вызовы и источники стратегий в международном киберзаконодательстве.

66. Основные российские правовые нормативные акты, касающиеся

кибербезопасности и определять ключевые правовые органы в рамках соответствующих организаций.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативно-правовые документы

1. ISO/IEC 27001:2013 Информационные технологии. Методы информационной безопасности. Системы управления информационной безопасностью. Требования

2. ISO/IEC 27005:2018 Информационные технологии. Методы информационной безопасности. Управление рисками информационной безопасности.

3. ISO/IEC 27031:2015 Информационные технологии. Методы информационной безопасности. Руководящие указания по готовности информационно-коммуникационных технологий для непрерывности ведения бизнеса.

4. ISO/IEC 27032:2012 Информационные технологии. Методы информационной безопасности. Руководящие указания по кибербезопасности.

Рекомендуемая литература:

а) основная литература:

5. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование:). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/1178150 (дата обращения: 19.09.2024). — Текст : электронный.

6. Овчинников, А. И. Основы национальной безопасности : учебное пособие / А. И. Овчинников, А. Ю. Мамычев, П. П. Баранов. — 2-е изд. — Москва : РИОР : ИНФРА-М, 2019. — 224 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: https://new.znanium.com/catalog/product/1012997 (дата обращения: 19.09.2024). - Текст : электронный.

7. Жук, А. П. Защита информации : учеб. пособие / А. П. Жук, Е. П. Жук, О.

М. Лепешкин [и др.]. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/2140566 (дата обращения: 19.09.2024). - Текст : электронный.

б) дополнительная литература:

8. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/2082642 (дата обращения: 19.09.2024). - Текст : электронный.

9. Ищейнов, В. Я. Основные положения информационной безопасности: учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва : ФОРУМ : ИНФРА-М, 2021. - 208 с. – ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/1189337 (дата обращения: 19.09.2024). - Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Федеральной службы по техническому и экспортному контролю www.fstec.ru
2. http://www.infosecurity. report.ru/
3. http://meganorm.ru/list/14-0.htm
4. http://dsbb.imf.org.
5. http://www.infoforum.ru/
6. http://www.iwars.su/
7. http://www.itsec.ru/main.php/
8. http://www.un.org/russian/online/loc1.htm.
9. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
10. Электронно-библиотечная система BOOK.RU http://www.book.ru
11. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
12. Электронно-библиотечная система Znanium http://www.znanium.com
13. Электронно-библиотечная система издательства «ЮРАЙТ» https://urait.ru/
14. Электронно-библиотечная система издательства Проспект http://ebs.prospekt.org/books
15. Электронно-библиотечная система издательства Лань https://e.lanbook.com/
16. Деловая онлайн-библиотека Alpina Digital http://lib.alpinadigital.ru/
17. Электронная библиотека Издательского дома «Гребенников»

https://grebennikon.ru/
18. Научная электронная библиотека eLibrary.ru http://elibrary.ru
19. Национальная электронная библиотека http://нэб.рф/
20. Финансовая справочная система «Финансовый директор» http://www.1fd.ru/
21. СПАРК https://spark-interfax.ru/
22. Библиотека онлайн Лекций по Бизнесу и Маркетингу издательства Henry Stewart Talks
23. CNKI. Academic Reference https://ar.oversea.cnki.net/
24. CNKI. China Academic Journals Full-text Database https://oversea.cnki.net/kns?dbcode=CFLQ
25. Электронные продукты издательства Elsevier http://www.sciencedirect.com
26. Коллекция научных журналов Oxford University Press https://academic.oup.com/journals/
27. Электронные коллекции книг и журналов издательства Springer: http://link.springer.com/
28. База данных научных журналов издательства Wiley https://onlinelibrary.wiley.com/

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11.1. Комплект лицензионного программного обеспечения

1. Astra Linux, Libre Office

2. Антивирус Kaspersky

11.2 Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»

2. Информационно-правовая система «Консультант Плюс»

3. Электронная энциклопедия: http://ru.wikipedia.org/wiki/Wiki

4. Система комплексного раскрытия информации «СКРИН» - http://www.skrin.ru/

11.3 Сертифицированные программные и аппаратные средства защиты информации

Программное средство анализа защищенности Средство анализа защищенности «Сканер-ВС»

Программно-аппаратный комплекс ПАК ViPNet Coordinator HW1000+IDS.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.