

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Департамент информационной безопасности

А.Н. Велигура

Управление информационной безопасностью

Рабочая программа дисциплины для студентов, обучающихся
по направлению подготовки
38.03.05 «Бизнес-информатика»,
Образовательная программа
«Цифровая трансформация управления бизнесом: ИТ-менеджмент в бизнесе»
«Технологии цифровых бизнес-моделей»

Москва
2021

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

**Департамент информационной безопасности
Факультет информационных технологий и анализа больших данных**

УТВЕРЖДАЮ

Проректор по учебной и
методической работе

_____ Е.А. Каменева

27.12. 2021 г.

А.Н. Велигура

Управление информационной безопасностью

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки

38.03.05 «Бизнес-информатика»,

Образовательная программа

«Цифровая трансформация управления бизнесом»

профили «ИТ-менеджмент в бизнесе»

«Технологии цифровых бизнес-моделей»

*Рекомендовано Ученым советом Факультета
информационных технологий и анализа больших данных
(протокол № 15 от 22.12.2021 г.)*

*Одобрено Советом учебно-научного Департамента информационной
безопасности
(протокол № 3 от 09.11. 2021 г.)*

Москва 2021

УДК 004.056.5
ББК 32.811.4
В27

Рецензент: д.т.н. профессор кафедры «Криптология и кибербезопасности»
НИЯУ МИФИ Иваненко В.Г.

А.Н. Велигура, «Управление информационной безопасностью».
Рабочая программа дисциплины для студентов, обучающихся по направлению 38.03.05 «Бизнес-информатика», Образовательная программа «Цифровая трансформация управления бизнесом» профили «ИТ-менеджмент в бизнесе» «Технологии цифровых бизнес-моделей» – М.: Финансовый университет, Департамент информационной безопасности, 2021 - 22.

Рабочая программа дисциплины содержит требования к результатам освоения дисциплины, содержание дисциплины, тематику практических занятий и технологии их проведения, формы самостоятельной работы, контрольные вопросы и систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

УДК 004.056.5

ББК 32.811.4

Учебное издание

Велигура Александр Николаевич

Управление информационной безопасностью

Рабочая программа дисциплины

Компьютерный набор, верстка

А.Н. Велигура

Формат 60х90/16. Гарнитура *Times New Roman*

Усл. п.л. 1,38. Изд. № _____. – 2021. Тираж - экз.

Заказ № _____

Отпечатано в Финансовом университете

© А.Н. Велигура, 2021

© Финансовый университет, 2021

СОДЕРЖАНИЕ

1. Наименование дисциплины	5
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине	5
3. Место дисциплины в структуре образовательной программы	6
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	7
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	7
5.1. Содержание тем дисциплины	7
5.2. Учебно-тематический план	10
5.3. Содержание семинаров, практических занятий	11
6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	12
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	12
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	12
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	14
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	18
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	20
10. Методические указания для обучающихся по освоению дисциплины	21
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	21
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	22

1. Наименование дисциплины

Управление информационной безопасностью

2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторам и достижения компетенции
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1.Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Знать основные требования к технике безопасности на рабочем месте, безопасным условиям труда. Уметь выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда
		2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знать основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах. Уметь проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.
		3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Знать основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества. Уметь находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной

			среды, обеспечения устойчивого развития общества.
		4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Знать основные способы выживания в экстремальных и чрезвычайных ситуациях. Уметь применять на практике основные способы выживания.
ПKN-12	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.
		2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» является обязательной дисциплиной цикла общепрофессиональных дисциплин направления 38.03.05 Бизнес-информатика, профили «ИТ-менеджмент в бизнесе», «Технологии цифровых бизнес-моделей»

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

Очная форма обучения

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 2 (в часах)
Общая трудоемкость дисциплины	4 з.е./144	144
Контактная работа-Аудиторные занятия	34	34
<i>Лекции</i>	16	16
<i>Семинары, практические занятия</i>	18	18
Самостоятельная работа	110	110
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 тем дисциплины

Раздел 1. Общие вопросы управления ИБ организации

Основные понятия, связанные с управлением ИБ Понятия: информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии и их роль в процессах управления ИБ. Угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ. Сущность управления ИБ организации Необходимость управления обеспечением ИБ организации. Процессный подход к управлению ИБ. Системный подход к управлению ИБ. Управление обеспечением ИБ организации как процесс. Циклическая модель PDCA применительно к управлению ИБ. Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Международная организация по стандартизации (ИСО, ISO). Международная электротехническая комиссия (МЭК, IEC). Национальные органы по стандартизации: Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Британский институт стандартов (BSI), Национальный институт стандартов и технологий США (NIST), Федеральное ведомство по безопасности информационных технологий (BSI, Германия). Общие сведения о стандартах США, Великобритании и Германии, касающихся вопросов управления ИБ. Комплекс стандартов и рекомендаций

Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Нормы и правила менеджмента ИБ. Цели и меры управления. Организация обеспечения информационной безопасности. Области контроля. Международные стандарты по общим вопросам управления ИБ (ISO 27001, ISO 27002, ISO 27003) и гармонизированные с ними российские национальные стандарты.

Раздел 2. Специальные вопросы управления ИБ организации

Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО БР ИББС. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и вопросы его использования. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Менеджмент риска информационной безопасности. Менеджмент инцидентов информационной безопасности. Обеспечение непрерывности деятельности и восстановления после прерываний. Обеспечение ИБ на стадиях жизненного цикла автоматизированных систем. Критерии оценки безопасности информационных технологий и автоматизированных систем.

Раздел 3. Реализация системы управления ИБ организации.

Планирование в управлении ИБ

Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков.

Внедрение системы управления информационной безопасностью

Разработка плана обработки рисков. Реализация плана обработки рисков для достижения намеченных целей управления. Внедрение мер управления, выбранные на стадии планирования, для достижения целей управления. Определение способа измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления. Реализация программы по обучению и повышению квалификации

сотрудников. Управление работой системой управления ИБ организации. Управление ресурсами системы управления ИБ организации. Внедрение процедур и других мер управления, обеспечивающих быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Анализ системы управления ИБ организации.

Выполнение процедуры мониторинга и анализа. Проведение регулярного анализа результативности системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ. Периодический пересмотр оценки рисков, анализ остаточных рисков и установленных приемлемых уровней рисков с учётом происходящих изменений. Проведение внутренних аудитов системы управления ИБ организации. Проведение руководством организации анализа системы управления ИБ организации для ее оценки и определения направлений совершенствования. Обновление планов обеспечения ИБ с учетом результатов анализа и мониторинга.

Совершенствование системы управления ИБ организации.

Выявление возможностей улучшения системы управления ИБ организации. Выполнение необходимых корректирующих и предупреждающих действий. Передача подробной информации о действиях по улучшению системы управления ИБ организации всем заинтересованным сторонам. Обеспечение внедрения улучшений системы управления ИБ организации для достижения запланированных целей.

Раздел 4. Внутренние нормативные документы по управлению ИБ организации.

Документационное обеспечение управления информационной безопасностью организации.

Задачи и назначение документационного обеспечения управления информационной безопасностью организации. Иерархия внутренних нормативных документов по управлению информационной безопасностью организации. Требования к организации документационного обеспечения управления информационной безопасностью организации.

Политика информационной безопасности организации. Роль политики ИБ как основного внутреннего нормативного документа по ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ

Другие документы по управлению ИБ.

Частные политики ИБ, их назначение и состав. Примеры областей обеспечения ИБ, управляемые частными политиками. Документы, содержащие

положения ИБ, применяемые к процедурам обеспечения ИБ. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ.

5.2. Учебно-тематический план

Таблица 3

№ п/п	Наименование разделов дисциплины,	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего часов	Аудиторная работа			Самостоя тельная работа	
			Общая	Лекции	Семинары, практические занятия		
1.	Общие вопросы управления ИБ организации	36	8	4	4	28	Доклады, презентации и дискуссии
2.	Специальные вопросы управления ИБ организации	36	10	4	6	26	Доклады, презентации и дискуссии
3.	Реализация системы управления ИБ организации.	36	8	4	4	28	Доклады, презентации и дискуссии
4.	Внутренние нормативные документы по управлению ИБ организации.	36	8	4	4	28	Доклады, презентации и дискуссии
	В целом по дисциплине	144	34	16	18	110	Согласно учебному плану контрольная работа
	Итого в %		24%	47%	53%	76%	

5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Общие вопросы управления ИБ организации	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Источники: 8.1,8.2,8.3	Групповые дискуссии презентация основных подходов. Учебное задание: сравнение подходов к управлению ИБ в ISO, России, США и Германии.
Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО и РС БР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний. Источники: 8.2,8.3, 8.4	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики ГОСТ Р 57580.2
Реализация системы управления ИБ организации.	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. Источники: 8.2,8.3, 8.5	групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики оценки модели угроз
Внутренние нормативные документы по управлению ИБ организации.	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению ИБ. Источники: 8.1,8.2,8.5	групповые дискуссии презентация основных подходов. Учебное задание: Пример составления частных политик

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

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

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы управления организации ИБ	Стандарты систем менеджмента качества в управлении ИБ	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Специальные вопросы управления организации ИБ	Положения ГОСТ Р 57580.1 в документах Банка России. Менеджмент инцидентов ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Реализация системы управления ИБ организации	Определение подхода к оценке риска в организации. Управление ресурсами системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Внутренние нормативные документы по управлению ИБ организации	Частные политики ИБ, их назначение и состав.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания

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

Основные формы текущего контроля:

- участие в дискуссиях по проблемным темам дисциплины;
- выступление с докладом по проблемным темам дисциплины;
- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, письменных работ, обсуждение и анализ их результатов.

Примерный перечень тем контрольных работ

1. Виды информации, подлежащей защите в РФ.
2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций
5. Ключевые требования к защите информации при осуществлении переводов денежных средств.
6. Методика оценки модели угроз и ее применение.
7. Ключевые субъекты НПС.

Примерный перечень вопросов для дискуссий

1. Национальная платежная система, ее участники и требования к обеспечению ИБ .
2. Менеджмент инцидентов ИБ.
3. Управление в инфраструктуре открытых ключей.
4. Мошеннические операции в кредитно-финансовой сфере.
5. Аудит ИБ

Примерный перечень тем докладов с презентациями

1. Международные и национальные российские стандарты по информационной безопасности.
2. Международные и национальные российские стандарты по управлению информационной безопасностью.
3. Регулирование ИБ международных карточных платежных систем.
4. Требования к обеспечению ИБ в РФ.
5. Требования к обеспечению ИБ в финансовых организациях РФ.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (экзамен) отводится 60

баллов. Распределение баллов по видам работ, формирующих текущий контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельной работы.

Критерии балльной оценки различных форм текущего контроля успеваемости

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Департамента информационной безопасности.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в разделе 2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине.

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

Таблица 6

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий,	1.Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Знать основные требования к технике безопасности на рабочем месте, безопасным условиям труда. Уметь выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте,	Составить план контроля соблюдения техники безопасности на рабочем месте

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенций	Типовые контрольные задания
катастроф, стихийных бедствий и военных конфликтов		обеспечивая безопасные условия труда	
	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знать основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах. Уметь проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Составить проект мероприятий по действиям в чрезвычайных ситуациях
	3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Знать основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества. Уметь находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Составить план проведения тренировок по действиям в чрезвычайных ситуациях
	4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Знать основные способы выживания в экстремальных и чрезвычайных ситуациях. Уметь применять на практике основные	Составить проект методических рекомендаций по применению на практике основных способов выживания.

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенций	Типовые контрольные задания
		способы выживания.	
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Составить аналитический обзор инфраструктурных решений центров обработки данных.
	2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Уметь формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций.

Примеры практико-ориентированных (ситуационных) заданий

Задача 1. Составьте модель угроз нарушения информационной безопасности для автоматизированной банковской системы коммерческого банка.

Задача 2. Составьте проект перечня событий ИБ для использования при

мониторинге и выявлении инцидентов ИБ.

Задача 3. В ходе проведенного службой информационной безопасности банка были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

Задача 4. В ходе проведенной службой информационной безопасности банка проверки было выявлено случаи накопления прав доступа работников при переходе в другие подразделения. Предложите способы недопущения таких событий.

Задача 5. В корпоративной сети кредитной организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.

Задача 6. Составьте развернутый план частной политики использования паролей.

Теоретические вопросы для подготовки к зачету

1. В чем основное отличие информационной безопасности от киберустойчивости?
2. Укажите основные государственные органы, требования которых по защите информации обязательны.
3. Что такое угроза (ИБ)?
4. Что такое уязвимость (в контексте ИБ) и к чему она относится?
5. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?
6. В чем заключаются особенности защиты коммерческой тайны?
7. Что такое инсайдерская информация с точки зрения закона «О противодействии неправомерному использованию инсайдерской информации...» (224-ФЗ)?

8. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ?
9. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?
10. На какие категории подразделяются персональные данные?
11. Что такое банковская тайна?
12. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?
13. Что такое идентификация и аутентификация?
14. Укажите типы факторов аутентификации.
15. Опишите основные угрозы аутентификации.
16. Укажите плюсы и минусы парольной аутентификации.

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

Нормативные акты

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности». [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.
2. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)». [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.
3. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.
4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.
5. Письмо Банка России от 24 мая 2005 г. №76-Т «Об организации управления операционным риском в кредитных организациях». [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.
6. Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и

банковской группе» [Электронный документ]. Режим доступа: URL: <http://www.consultant.ru/>.

7. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014.

8. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: <http://www.27000.org/>.

9. ГОСТ Р ИСО ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности.

10. ГОСТ Р 57580.1 – 2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Рекомендуемая литература:

а) основная:

1. Курило, А. П. Вопросы управления информационной безопасностью. Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. – Москва : Горячая линия-Телеком, 2013. – 244 с. – ЭБС ZNANIUM.com. – URL: <http://znanium.com/catalog/product/560780> (дата обращения: 7.12.2021). – Текст: электронный.

2. Милославская, Н. Г. Вопросы управления информационной безопасностью. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия-Телеком, 2013. – 130 с. – ЭБС ZNANIUM.com. – URL: <http://znanium.com/catalog/product/560781> (дата обращения: 7.12.2021). – Текст : электронный.

3. Милославская Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е изд. – Москва : Горячая линия-Телеком, 2016. – 170 с. – ЭБС ZNANIUM.com. – URL: <https://znanium.com/catalog/product/560782> (дата обращения: 7.12.2021). – Текст: электронный.

4. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия-

Телеком, 2013. – 214 с. – ЭБС ZNANIUM.com. – URL: <http://znanium.com/catalog/product/560783> (дата обращения: 7.12.2021). – Текст : электронный.

б) дополнительная:

5. Воронцова, С. В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок) : монография / С. В. Воронцова. — Москва : КноРус, 2021. — 159 с. - ЭБС BOOK.ru. — URL: <https://book.ru/book/940132> (дата обращения: 7.12.2021). — Текст : электронный.

6. Милославская Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва: Горячая линия-Телеком, 2013. – 166 с. - ЭБС ZNANIUM.com. – URL: <http://znanium.com/catalog.php?bookinfo=560784> (дата обращения: 7.12.2021). - Текст: электронный.

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

1. Сайт Центрального банка Российской Федерации: www.cbr.ru.
2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru.
3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>.
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>.
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>.
7. Электронно-библиотечная система Znanium <http://www.znanium.com>.
8. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
9. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>.

10. Электронно-библиотечная система издательства «Лань»
<https://e.lanbook.com/>.
11. Электронная библиотека Издательского дома «Гребенников»
<https://grebennikon.ru/>.
12. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>.
13. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>.
14. Национальная электронная библиотека <http://нэб.рф/>.
15. Academic Reference <http://ar.cnki.net/ACADREF>.
16. Пакет баз данных компании EBSCO Publishing, крупнейшего агрегатора научных ресурсов ведущих издательств мира <http://search.ebscohost.com>.
17. Электронные продукты издательства Elsevier
<http://www.sciencedirect.com>.
18. Emerald: Management eJournal Portfolio <https://www.emerald.com/insight/>.
19. Oxford Scholarship Online <https://oxford.universitypressscholarship.com/>.
20. Коллекция научных журналов Oxford University Press
<https://academic.oup.com/journals/>.
21. ProQuest: База данных Business Ebook Subscription на платформе Ebook Central <https://search.proquest.com/>.
22. ProQuest Dissertations & Theses A&I <https://search.proquest.com/>.
23. Scopus <https://www.scopus.com>.
24. Электронная коллекция книг издательства Springer: Springer eBooks
<http://link.springer.com/>.
25. Web of Science <http://apps.webofknowledge.com>.

10. Методические указания для обучающихся по освоению дисциплины

Студентам при подготовке следует использовать нормативные документы Финансового университета, а именно, - Примерные методические рекомендации для студентов по освоению дисциплин образовательных программ высшего образования в соответствии с распоряжением

Финуниверситета от № 1040/о от 11.05.2021 (см. сайт Финансового Университета: на главной странице раздел «Наш университет»; далее «Единая правовая база Финуниверситета»; подраздел «Методическая работа» - «Распоряжения»/«Приказы Финуниверситета»), использовать методические рекомендации департаментов и кафедр.

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:

Windows, Microsoft Office
антивирус ESET Endpoint Security

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:

Не предусмотрены.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

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

**ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Курский филиал федерального государственного образовательного бюджетного
учреждения высшего образования
Кафедра «Менеджмента и информационных технологий»

УТВЕРЖДАЮ

Директор филиала

_____ Ю.В. Вертакова
« ____ » _____ 20 ____ г.

Приложение к рабочей программе дисциплины

Управление информационной безопасностью

Направление подготовки 38.03.05 «Бизнес-информатика»

Профиль «ИТ менеджмент в бизнесе»

Год утверждения программы: 2021

Одобрено кафедрой «Менеджмент и информационные технологии»

Протокол от « 31 » 08.2021 г. №1

Курск 2021

1. Наименование дисциплины

Управление информационной безопасностью

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

Направление подготовки 38.03.05 «Бизнес-информатика». Форма обучения: очно- заочная 2021 год приема

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда. 2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях. 3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей. 4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания.	Знать способы выявления и устранения проблем, связанных с нарушениями техники безопасности на рабочем месте, обеспечения безопасных условий труда. Уметь выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда. Знать мероприятия по защите населения и территорий в чрезвычайных ситуациях Уметь осуществлять выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях Знать пути решения ситуаций, связанных с безопасностью жизнедеятельности людей Уметь находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей. Знать основные способы выживания в экстремальных и чрезвычайных ситуациях. Уметь действовать в экстремальных и чрезвычайных ситуациях, применять на практике основные способы выживания.
ПKN- 12	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. 2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знать методику проведения анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Уметь проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Знать системы хранения данных и инфраструктурных решений центров обработки данных, способы использования вычислительного оборудования. Уметь оказывать консультацию по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.

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

Направление подготовки 38.03.05 «Бизнес-информатика». Форма обучения: очная, очно-заочная 2021 год приема

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 4 (в часах)
Общая трудоемкость дисциплины	4 з.е., 144 ч	4 з.е., 144 ч
<i>Контактная работа - Аудиторные занятия</i>	16	16
<i>Лекции</i>	4	4
<i>Семинары, практические занятия</i>	12	12
<i>Самостоятельная работа</i>	128	128
Вид текущего контроля	<i>РАР</i>	<i>РАР</i>
Вид промежуточной аттестации	<i>Зачет</i>	<i>Зачет</i>

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

5.1. Содержание тем дисциплины

Раздел 1. Информационная безопасность в системе национальной безопасности

Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности.

Раздел 2. Информационные уязвимости объектов

Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости.

Раздел 3. Угрозы информационной безопасности и их источники

Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности.

Раздел 4. Средства обеспечения информационной безопасности

Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Раздел 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации

Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.

Раздел 6. Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей

Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное,

прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно-вычислительная система. Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации. Развитие идей и концепций защиты информации в банках.

5.2. Учебно-тематический план

№ п/ п	Наименование разделов дисциплины,	Трудоемкость в часах						Формы текущего контроля успеваемости
		Все го час ов	Аудиторная работа				Само стоят ельна я работ а	
			Об щая	Лек ции	Семина ры, практич еские занятия	Занятия в интерак тивных формах		
1.	Информационная безопасность в системе национальной безопасности	24	2,5	0,5	2		21,5	Доклады, презентации, обсуждение в группе, опрос
2.	Информационные уязвимости объектов	24	2,5	0,5	2		21,5	Доклады, презентации, обсуждение в группе
3.	Угрозы информационной безопасности и их источники	24	2,5	0,5	2		21,5	Доклады, презентации, обсуждение в группе, опрос
4.	Средства обеспечения информационной безопасности	24	2,5	0,5	2		21,5	Доклады, презентации, обсуждение в группе
5.	Риски информационной безопасности и проблема построения комплексной системы защиты информации	24	2,5	0,5	2		21,5	Доклады, презентации, обсуждение в группе, опрос
6.	Обработка и передача информации в вычислительных и управляющих системах банков и сетях связи, вопросы информационной безопасности и	24	3,5	1,5	2		20,5	Доклады, презентации, обсуждение в группе

защиты информации для вычислительных и управляющих систем и сетей							
В целом по дисциплине	144	16	4	12		128	Согласно учебному плану: контрольная работа

5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9	Формы проведения занятий
1.Понятийный аппарат и основы терминологии информационной и национальной безопасности. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности.	1. Основные подходы к определению понятия "информационная безопасность". 2. Подходы к классификации угроз безопасности информации. 3. Методы практического обеспечения защиты информации корпоративных систем. 4. Направления политики информационной безопасности предприятия. 5. Проблемы защиты информации в Интернет. 4, 5, 9, 9. (6)	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Изучение профессиональной терминологии в области информационной безопасности и информационного противоборства. Моделирование наиболее эффективного решения проблемы обеспечения информационной безопасности.
2.Организационно-правовые и комбинированные информационные уязвимости.	1. Основные положения законодательных актов России по информационной безопасности. 2. Руководящие документы ФСТЭК. 3. Основные подходы к аудиту информационной безопасности предприятия. 4. Государственные и международные стандарты в области информационной безопасности. 5. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности. 6. Принципы организации работ с информацией, составляющей коммерческую тайну. 1, 2, 5, 8, 9. (1)	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Применение математического аппарата в профессиональной деятельности при выявлении сущности проблем, возникающих в задачах обеспечения информационной безопасности. Анализ конкретных правовых актов в области информационной безопасности.
3.Эндогенные и экзогенные, антропогенные и техногенные угрозы	1. Подходы к классификации угроз угрозы информации по степени защиты. 2. Уязвимости электронного	Групповые дискуссии, мозговой штурм, презентация основных подходов.

информационной безопасности, их классификация.	документооборота. 3. Основные принципы системной классификации угроз безопасности информации. 4. Риски при идентификации и аутентификации пользователей. 5. Риски утечки акустической информации. 6. Риски утечки информации по техническим каналам. 6, 10, 9. (3)	Учебное задание: Моделирование видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
4. Программно-аппаратные, криптографические и стеганографические средства защиты информации.	1. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях. 2. Определение криптографии, ее методы и алгоритмы. 3. Определение стеганография, ее достоинства и недостатки. 4. Системы криптографической защиты информации в России. 5. Специфика программно-аппаратных, криптографических средств защиты информации банковских карт. 7, 10, 9. (5)	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование способов противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.
5. Оценка рисков и организация управления процессом защиты информации.	1. Основные подходы к оценке рисков атак на информационные системы. 2. Типы компьютерных вирусов и специфических для них рисков. 3. Модели оценки рисков. 4. Наиболее актуальные подходы к управлению процессом защиты информации. 5. Наиболее значимые нормативные документы, регулирующие процессы управления защитой информации. 3, 5, 10, 9. (4)	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Разработка методики оценки информационных рисков, ее обсуждение и экспертная оценка.
6. Угрозы безопасности информации, обрабатываемой в компьютерных банковских системах.	1. Специфика рисков банковских угроз информационной безопасности. 2. Типы угроз банковской безопасности. 3. Наиболее уязвимые для банков каналы передачи информации. 4. Основные методы защиты от перехвата информации в банковских системах. 3. Перспективы использования блокчейна для защиты банковской информации. 6, 8, 9. (2)	Групповые дискуссии, мозговой штурм, презентация основных подходов. Учебное задание: Моделирование возможных каналов перехвата при передаче информации системами связи (электромагнитные, электрические, индукционные) и разработка способов их защиты.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

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

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
1.Понятийный аппарат и основы терминологии информационной и национальной безопасности. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности.	1. Основные проблемы информационной безопасности. 2. Смысл понятия «технический канал утечки информации». 3. Методы защиты от утечки информации по акустическому каналу. 4. Основные положения Доктрины информационной безопасности РФ. 5. Закон, определяющий техническое регулирование.	- работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
2.Организационно-правовые и комбинированные информационные уязвимости.	1.Защита информации в деловой переписке. 2. Особенности системы государственного управления Российской Федерации в области обеспечения информационной безопасности. 3. Основное содержание деятельности ФСТЭК и ФСБ России в области обеспечения информационной безопасности. 4. Особенности сертификации в области информационной безопасности РФ. 5. Функции и структура государственной системы обеспечения информационной безопасности.	- работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; - подготовка презентаций по теме.
3.Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.	1. Особенности защиты информации в вычислительных сетях. 2. Особенности лицензирования в области информационной безопасности РФ. 3. Специфика организации обучения и инструктирования сотрудников правилам работы с конфиденциальной информацией. 4. Техногенные угрозы информационной безопасности. 5. Угрозы информационной безопасности, связанные с	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.

	человеческим фактором.	
4. Программно-аппаратные, криптографические и стеганографические средства защиты информации.	1. Отличие криптографии от криптоанализа. 2. Законодательные акты, регулирующие электронную подпись. 3. Инфраструктура электронной подписи. 4. Основные способы аутентификации. 5. Методы криптографического закрытия информации. 6. Особенности отечественного стандарта шифрования.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
5. Оценка рисков и организация управления процессом защиты информации.	1. Экономика предприятия и информационная безопасность. 2. Задачи службы безопасности организации. 3. Информационные риски организации. 4. Стратегии снижения рисковозависимости предприятия в процессе управления. 5. Характер оценивая информационных рисков в процессе управления предприятием.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.
6. Угрозы безопасности информации, обрабатываемой в компьютерных банковских системах.	1. Элементы комплексной системы информационной безопасности предприятия. 2. Методы защиты информации техническими средствами в каналах связи банков. 3. Организационные источники и каналы утечки информации в банках. 4. Условия проверки на полиграфе в финансовых организациях. 5. Особенности организации защиты информации в кадровой службе.	-работа с учебной, научной и справочной литературой; -подготовка рефератов по теме; -подготовка презентаций по теме.

Примерный перечень вопросов к контрольной работе, примеры заданий контрольных работ

1. Социальная значимость специалиста в области информационной безопасности
2. Современные угрозы интересам личности и обеспечение информационной безопасности

3. Информационные войны: особенности их ведения в современном мире
4. Проблема разработки «Этического кодекса» специалиста в области информационной безопасности
5. Особенности профессиональной коммуникации в информационном обществе
6. Основные пути формирования толерантности у специалиста в области информационной безопасности
7. Национально-культурная специфика «хакерства» как субкультуры
8. Социально-психологический портрет инсайдера в области информационной безопасности
9. Математика и криптография: основные тенденции развития
10. Современная конкурентная разведка и ее возможности
11. Правовые проблемы информационной безопасности
12. Big Data и информационная безопасность
13. Современные дискуссии о копирайте
14. Трудности внедрения электронной цифровой подписи в России
15. Проблемы обеспечения информационной безопасности систем электронного правительства
16. «Темный Интернет»: перспективы и опасности его развития
17. Квантовые компьютеры и перспективы развития информационной безопасности
18. Возможности современных интеллектуальных систем (ИИ) в обеспечении информационной безопасности
19. Криптовалюты и информационная безопасность
20. Значение развития технологий блокчейна для информационной безопасности
21. Социально-психологические и личностные характеристики специалиста по защите информации

22. Профилактические меры по предотвращению компьютерной преступности

23. Биометрия в банковских системах и проблемы обеспечения информационной безопасности

24. Нейросети и возможности их использования для выявления угроз информационной безопасности

25. Самообучающиеся информационные системы и возможности их использования в информационной безопасности

Примерный перечень вопросов к аудиторной письменной работе

1. «Глубокая паутина»: перспективы и опасности его развития.
2. Новые социальные сетевые технологии и информационная безопасность.
3. Проблемы обеспечения информационной безопасности в банковских системах.
4. Искусственный интеллект и информационная безопасность.
5. Блокчейна и информационная безопасность
6. Основные подходы к эффективному ведению информационных войн.
7. Перспективы развития информационной безопасности в XXI веке.
8. Электронные деньги и проблемы информационной безопасности.
9. Математические методы в криптографии.
10. Типология и национально-психологические особенности хакеров.
11. Нейросети в информационной безопасности
12. Этический кодекс специалиста в области информационной безопасности
13. Профессиональные сообщества и информационная безопасность
14. Информационная безопасность
15. Этика специалиста в области информационной безопасности
16. Электронное правительство и информационная безопасность
17. Виды компьютерной преступности компьютерной преступности
18. Эволюция информационных систем и информационной безопасности

19. Контент - анализ и информационная безопасность
20. Копирайт и информационная безопасность
21. Личность и ее информационная безопасность.
22. Значение информационной безопасности в развитии общества.
23. Требования к специалисту по защите информации
24. Инсайдинг и информационная безопасность.
25. Электронная подпись и информационная безопасность.

**Примерный перечень докладов и презентаций по проблемным
темам дисциплины**

1. Проблема определения понятия «информационный риск».
2. Специфика информационного риска в рискологии.
3. Проблема количественного измерения информационного риска.
4. Основные подходы к определению качественной специфики информационного риска.
5. Специфика рисков информационной безопасности в России
6. Специфика рисков информационной безопасности в Китае
7. Специфика рисков информационной безопасности в США
8. Специфика рисков информационной безопасности в Индии
9. Специфика рисков информационной безопасности в Англии
10. Специфика рисков информационной безопасности во Франции
11. Специфика рисков информационной безопасности в Германии
12. Особенности рисков информационной безопасности в Японии
13. Специфика рисков информационной безопасности в Канаде
14. Специфика рисков информационной безопасности в Австралии
15. Особенности хакерской активности в Канаде
16. Особенности хакерской активности в Австралии
17. Особенности хакерской активности в России
18. Особенности хакерской активности в Японии
19. Особенности хакерской активности в Германии
20. Особенности хакерской активности в Китае

21. Особенности хакерской активности в Англии
22. Особенности хакерской активности во Франции
23. Особенности хакерской активности в США
24. Особенности хакерской активности в Индии
25. Проблема использования новых социальных сетевых технологий при оценке информационных рисков.

**Примерный перечень тематики учебных практических заданий
(лабораторных работ)**

1. Основные подходы к определению понятия "информационная безопасность".
2. Подходы к классификации угроз безопасности информации.
3. Методы практического обеспечения защиты информации корпоративных систем.
4. Направления политики информационной безопасности предприятия.
5. Проблемы защиты информации в Интернет.
6. Основные положения законодательных актов России по информационной безопасности.
7. Руководящие документы ФСТЭК России.
8. Основные подходы к аудиту информационной безопасности предприятия.
9. Государственные и международные стандарты в области информационной безопасности.
10. Проблемы взаимосвязи этики и правосудия при обеспечении информационной безопасности.
11. Принципы организации работ с информацией, составляющей коммерческую тайну.
12. Подходы к классификации угроз угрозы информации по степени защиты.
13. Уязвимости электронного документооборота.

14. Основные принципы системной классификации угроз безопасности информации.
15. Риски при идентификации и аутентификации пользователей.
16. Риски утечки акустической информации.
17. Риски утечки информации по техническим каналам.
18. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях.
19. Определение криптографии, ее методы и алгоритмы.
20. Определение стеганография, ее достоинства и недостатки.
21. Системы криптографической защиты информации в России.
22. Специфика программно-аппаратных, криптографических средств защиты информации банковских карт.
23. Основные подходы к оценке рисков атак на информационные системы.
24. Типы компьютерных вирусов и специфических для них рисков.
25. Модели оценки рисков.
26. Наиболее актуальные подходы к управлению процессом защиты информации.
27. Наиболее значимые нормативные документы, регулирующие процессы управления защитой информации.
28. Специфика рисков банковских угроз информационной безопасности.
29. Типы угроз банковской безопасности.
30. Наиболее уязвимые для банков каналы передачи информации.
31. Основные методы защиты от перехвата информации в банковских системах.
32. Перспективы использования блокчейна для защиты банковской информации.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (зачет) отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий

контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельной работы. Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры «Информационная безопасность».

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в Разделе 2. «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».

Для 2020 года приема

компетенция	типовые задания
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий	Индикатор 1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда. Знает способы выявления и устранения проблем, связанных с нарушениями техники безопасности на рабочем месте, обеспечения безопасных условий труда Задание 1. Выбрать наиболее эффективные средства сбора необходимой информации для решения задач обеспечения безопасных условий труда информационной безопасности Задание 2. Провести анализ возможных стратегий сбора информации для решения профессиональных задач информационной безопасности Умеет выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечения безопасных условий труда Задание 1. Выявить алгоритм решения проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечения информационной безопасности Задание 2. Представить методику проверки у специалистов осведомленности о технике безопасности и подходы к устранению недостатков. Индикатор 2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях. Знает мероприятия по защите населения и территорий в чрезвычайных ситуациях Задание 1 Читать литературу по защите населения и территорий

	в чрезвычайных ситуациях Задание 2 Систематизировать мероприятия по защите населения и территорий в чрезвычайных ситуациях Умеет осуществлять выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях Задание 1 Выделить комплекс актуальных мероприятий по защите населения и территорий в чрезвычайных ситуациях Задание 2 Создать аналитическую записку, отражающую систему мероприятий по защите населения и территорий в чрезвычайных ситуациях. Индикатор 3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей. Знает пути решения ситуаций, связанных с безопасностью жизнедеятельности людей Задание 1 Изучить литературу, связанную с безопасностью жизнедеятельности людей Задание 2 Освоить терминологию в области безопасности жизнедеятельности людей Умеет находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей. Задание 1 Найти пути решения ситуаций, связанных с безопасностью жизнедеятельности людей в отечественной литературе. Задание 2 Структурировать пути решения ситуаций, связанных с безопасностью жизнедеятельности людей в отечественной литературе. Индикатор 4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания. Знает основные способы выживания в экстремальных и чрезвычайных ситуациях. Задание 1. Выделить основные способы выживания, действуя в экстремальных и чрезвычайных ситуациях. Задание 2. Найти наиболее эффективные подходы к разрешению экстремальных и чрезвычайных ситуаций. Умеет действовать в экстремальных и чрезвычайных ситуациях, применять на практике основные способы выживания. Задание 1. Представить и охарактеризовать алгоритм действия в экстремальных и чрезвычайных ситуациях. Задание 2. Выделить наиболее эффективные способы выживания в зависимости от специфики экстремальных и чрезвычайных ситуаций.
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и	Индикатор 1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Знает методику проведения анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных

инфраструктурные решения центров обработки данных	решений центров обработки данных. Задание 1. Представить методику анализа рынка вычислительного оборудования и систем хранения данных с позиций информационной безопасности. Задание 2. Выделить наиболее эффективные подходы к принятию инфраструктурных решений центров обработки данных в области информационной безопасности. Умеет поводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Задание 1. Провести анализ рынка вычислительного оборудования и систем хранения данных с позиций информационной безопасности. Задание 2. Провести анализ инфраструктурных решений центров обработки данных в области информационной безопасности. Индикатор 2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Знает системы хранения данных и инфраструктурных решений центров обработки данных, способы использования вычислительного оборудования. Задание 1. Охарактеризовать системы хранения данных и инфраструктурных решений центров обработки данных. Задание 2. Выделить наиболее эффективные способы использования вычислительного оборудования. Умеет оказывать консультацию по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. Задание 1. Представить алгоритм консультации по использованию вычислительного оборудования и систем хранения данных в области информационной безопасности. Задание 2. Представить алгоритм консультации по принятию инфраструктурных решений центров обработки данных с учетом информационной безопасности.
--	---

Примерный перечень вопросов к зачету

1. Какие вам известны подходы к классификации угроз безопасности информации?
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

3. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

4. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

5. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

6. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

7. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

8. Охарактеризуйте проблему определения предметной области информационной безопасности.

9. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

10. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

11. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

12. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.

13. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

14. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

15. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
16. Объясните, что представляет собой стеганография?
17. Расскажите об особенностях симметричных и несимметричных шифров.
18. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?
19. Охарактеризуйте наиболее известный алгоритм шифрования DES.
20. Каковы основные особенности криптосистем с общедоступным ключом?
21. Раскройте основное содержание алгоритма электронной цифровой подписи.
22. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.
23. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
24. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.
25. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
26. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?
27. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
28. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.
29. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

30. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

31. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

32. Дайте классификацию источников утечки информации по техническим каналам.

33. Назовите известные вам методы и средства контроля акустической информации.

34. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

35. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

36. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

37. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

38. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.

39. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

40. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

41. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

42. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

43. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

44. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

45. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

46. Интеллектуальная банковская карта, ее защита.

47. Меры наказания за противозаконные деяния в сфере платежных карт.

48. Меры предосторожности при использовании банкоматов.

49. Меры предосторожности при оплате картой покупок в Интернете.

50. Базовый набор требований к системе ИБ организаций БС РФ.

Примеры тестовых заданий

Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство:

- a. доступность
- b. детерминированность
- c. восстанавливаемость
- d. целостность.

Действие программных закладок основывается на инициировании или

подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели:

- a. искажение
- b. наблюдение
- c. компрометация
- d. перехват.

Длина исходного ключа у алгоритма шифрования DES (бит)

- a. 56
- b. 128
- c. 64
- d. 256.

Защита информации это:

- a. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- b. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- c. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- d. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё. Обоснуйте ваш выбор.

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

- a. активный перехват;
- b. пассивный перехват;
- c. аудиоперехват;
- d. исследования.

Примеры практико-ориентированных (ситуационных) заданий

1. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации?

2. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.

3. Рассмотрите возможности несанкционированного получения информации в следующем случае:

- в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;
- объектами несанкционированных действий, являются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;
- каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача ее на печать.

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

4. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

5. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.