

Федеральное государственное образовательное бюджетное учреждение
высшего образования

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

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

Резниченко С.А.

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
2022

Федеральное государственное образовательное бюджетное учреждение
высшего образования

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

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

УТВЕРЖДАЮ

Проректор по учебной
и методической работе

_____ Е.А. Каменева

«19» декабря 2022г.

Резниченко С.А.

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»

*Рекомендовано методической комиссией Факультета
информационных технологий и анализа больших данных
(протокол № 27 от 15.12. 2022 г.)*

*Одобрено Советом учебно-научного Департамента информационной
безопасности
(протокол № 13 от 13.12.2022 г.)*

Москва 2022

СОДЕРЖАНИЕ

1. Наименование дисциплины	4
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине	4
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	8
5.3. Содержание семинаров, практических занятий	9
6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	10
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	10
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	11
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	12
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	16
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	Ошибка! Залка не определена.
10. Методические указания для обучающихся по освоению дисциплины	19
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	19
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	29

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

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
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.
		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.
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности и для сохранения природной среды, обеспечения	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,

	устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, 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.
		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.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к Модулю общепрофессиональных дисциплин учебного плана направления подготовки бакалавриата 38.03.05 Бизнес-информатика, образовательной программы «Цифровая трансформация управления бизнесом» профилей «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

Таблица 1

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Модуль 3 (в часах)
Общая трудоёмкость дисциплины	4 з.е./144	144
Контактная работа-Аудиторные занятия	50	50
<i>Лекции</i>	16	16
<i>Семинары, практические занятия в т.ч.</i>	34	34
Самостоятельная работа	94	94
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

Тема 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, 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.

Тема 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.

Тема 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.

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.

Тема 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 2

№ п/п	Наименование разделов дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
			Общая	Лекции	Семинары, практические занятия	Самостоятельная работа	
1.	Общие вопросы управления ИБ организации	36	10	4	8	22	Доклады, презентации и дискуссии
2.	Специальные вопросы управления ИБ организации	36	10	4	8	22	Доклады, презентации и дискуссии

3.	Реализация системы управления ИБ организации.	36	14	4	8	24	Доклады, презентации и дискуссии
4.	Внутренние нормативные документы по управлению ИБ организации.	36	16	4	10	26	Доклады, презентации и дискуссии
	В целом по дисциплине	144	50	16	34	94	Согласно учебному плану контрольная работа
	Итого в %		35%	32%	68%	65%	

5.3. Содержание семинаров, практических занятий

Таблица 3

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 4

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы Управления ИБ организации	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 ИБ организации	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	Частные политики ИБ, их назначение и состав.	- работа с учебной, научной и справочной литературой;

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
документы по управлению ИБ организации		<ul style="list-style-type: none"> - 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 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 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с 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, катастроф, стихийных бедствий и военных конфликтов	Индикатор 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	Задание 1 Составить план контроля соблюдения техники безопасности на рабочем месте Задание 2 Продemonстрировать методы повышения эффективности собственной деятельности
	Индикатор 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.	Задание 1 Составить план контроля соблюдения техники безопасности на рабочем месте Задание 2 Продemonстрировать методы повышения эффективности собственной деятельности
	Индикатор 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.	Задание 1 Составить план контроля соблюдения техники безопасности на рабочем месте Задание 2 Составить план мероприятий по действиям в ходе военного конфликта
	Индикатор 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.	Задание 1 Составить план проведения тренировок по действиям при наводнении Задание 2 Составить план проведения тренировок по

			действия при пожаре
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	Индикатор 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.	Задание 1 Составить аналитический обзор инфраструктурных решений центров обработки данных. Задание 2 Проанализировать рынок вычислительного оборудования, систем хранения данных.
	Индикатор 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.	Задание 1 Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций. Задание 2 Сформулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений

Примеры практико-ориентированных (ситуационных) заданий

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

Задача 2. Составьте проект классификатора инцидентов ИБ.

Задача 3. Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1.

Задача 4. В ходе проведенной службой информационной безопасности банка проверки были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

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 менеджмента инцидентов ИБ.

Теоретические вопросы для подготовки к зачету

1. Какие действия и процессы составляют стадию проверки СУИБ?
2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?
3. Что такое информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии, киберустойчивость (в финансовой сфере)?
4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?
5. На какие категории подразделяются персональные данные?
6. Что такое банковская тайна?
7. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?
8. Что такое идентификация и аутентификация?
9. В чем заключается процессный подход к управлению ИБ?
10. Какие действия и процессы составляют стадию планирования СУИБ?
11. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?
12. Что такое циклическая модель PDCA применительно к управлению ИБ?
13. Что включает выбор и применение финансовой организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?
14. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование компенсирующих мер ЗИ? Какие условия при этом должны быть выполнены?
15. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р 57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ финансовой организации для конкретного контура безопасности?
16. Укажите стадии жизненного цикла автоматизированных систем. Чем

обусловлены особенностями обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

17. Назовите основные нормативно правовые документы в области управления информационной безопасности.

18. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ?

19. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?

20. Укажите типы факторов аутентификации.

21. Опишите основные угрозы аутентификации.

22. Укажите плюсы и минусы парольной аутентификации.

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

Нормативные акты

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (В редакции от 02.07.2021 г.).

2. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне» (В редакции от 11.06.2021 г.)

3. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (В редакции от 09.03.2021 г.).

4. Распоряжение Правительства России от 28 июля 2017 г. №1632-р «Об утверждении Программы «Цифровая экономика Российской Федерации»

5. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7. ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
8. ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
9. ГОСТ Р 50922 Защита информации. Основные термины и определения.
10. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
11. ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
12. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.
13. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
14. ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
15. ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
16. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
17. ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
18. ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

19. ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

Рекомендуемая литература:

а) основная:

1. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола : Поволжский государственный технологический университет, 2020. - 154 с. – ЭБС ZNANIUM.com. - URL: <https://znanium.com/catalog/product/1894130> (дата обращения: 03.04.2023). – Текст: электронный.

2. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. – ЭБС ZNANIUM.com. - URL: <https://znanium.com/catalog/product/1021744> (дата обращения: 03.04.2023). – Текст: электронный.

б) дополнительная:

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: 03.04.2023). - 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/>.

10. Методические указания для обучающихся по освоению дисциплины

Студентам при подготовке следует использовать нормативные документы Финансового университета, а именно, - «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете» от 11.05.2021 № 1040/о (см. сайт Финансового Университета: на главной странице раздел «Наш университет»; далее «Единая правовая база Финуниверситета»; подраздел «Методическая работа» - «Распоряжения»/«Приказы Финуниверситета»), использовать методические рекомендации департамента информационной безопасности.

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 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:

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.