

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.
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.

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 и 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 и индикаторами достижения компетенций	Типовые контрольные задания
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.	способы выживания. 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.