ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Директор/Декан
института экономики, финансов и управления в АПК
Гунько Юлия Александровна

_____

_____

«___» _____ 20___ г.

Рабочая программа дисциплины

Б1.В.03 Кибербезопасность в финансовой системе

38.04.01 Экономика

Финансовый контроль и цифровизация экономической деятельности

магистр

заочная

Ставрополь, 2026

1. Цель дисциплины

Целью освоения дисциплины «Кибербезопасность в финансовой системе» является формирование у обучающихся знаний и практических навыков обеспечения кибербезопасности в финансовой системе, включая внедрение цифровых систем финансового контроля и внутреннего аудита с учётом требований кибербезопасности.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-2 Способен организовать разработку и утвердить отчетные документы о работе системы внутреннего контроля экономического субъекта	ПК-2.2 Способность осуществлять внедрение цифровых систем финансового контроля и внутреннего аудита с учётом требований кибербезопасности для организаций	**знает** Знает угрозы кибербезопасности в финансовой системе, цифровые системы финансового контроля и внутреннего аудита, требования кибербезопасности. **умеет** Умеет осуществлять внедрение цифровых систем финансового контроля и внутреннего аудита с учётом требований кибербезопасности. **владеет навыками** Владеет навыками обеспечения кибербезопасности при внедрении цифровых систем финансового контроля в финансовой системе.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность в финансовой системе» является дисциплиной части, формируемой участниками образовательных отношений программы.

Изучение дисциплины осуществляется в 2 курсе (-ах).

Для освоения дисциплины «Кибербезопасность в финансовой системе» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин:

Ознакомительная практика

Практика по профилю профессиональной деятельности

Аудит

Компьютерные технологии в профессиональной деятельности

Освоение дисциплины «Кибербезопасность в финансовой системе» является необходимой основой для последующего изучения следующих дисциплин:

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Кибербезопасность в финансовой системе» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

Курс	Трудоемк	Контактная работа с преподавателем, час	Самостоя-	Контроль,	Форма

	ость час/з.е.	лек-ции	практические занятия	лабораторные занятия	тельная работа, час	час	промежуточной аттестации (форма контроля)
2	108/3	4	6		94	4	За
в т.ч. часов: в интерактивной форме		2	2				
практической подготовки		4	6		58		

Курс	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел					
		Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
2	108/3			0.12			

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

№	Наименование раздела/темы	Курс	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
			всего	Лекции	Семинарские занятия		Самостоятельная работа			
					Практические	Лабораторные				
1.	1 раздел. Раздел 1									
1.1.	ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ФИНАНСОВОЙ СФЕРЕ	2	2	2			18	КТ 1	Тест	ПК-2.2
1.2.	АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	2					40		Устный опрос	ПК-2.2
1.3.	УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	2	8	2	6		36	КТ 2	Тест	ПК-2.2
	Промежуточная аттестация	За								
	Итого		108	4	6		94			
	Итого		108	4	6		94			

5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий

Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/ (практическая подготовка)	Содержание темы (и/или раздела)	Всего, часов / часов интерактивных занятий/ практическая подготовка
ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И НОРМАТИВНО-	Финансовая кибербезопасность как системная категория	2/2

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ФИНАНСОВОЙ СФЕРЕ		
АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	Классификация угроз и моделирование нарушителя в финансовом секторе	/-
АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	Технологии защиты банковских информационных систем	/-
УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	Управление рисками информационной безопасности и операционная надежность	/-
УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	Аудит и оценка соответствия информационной безопасности	2/-
Итого		4

5.2.1. Семинарские (практические) занятия с указанием видов проведения занятий в интерактивной форме

Наименование раздела дисциплины	Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка)	Всего, часов / часов интерактивных занятий/ практическая подготовка	
		вид	часы
ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ФИНАНСОВОЙ СФЕРЕ	Вводный практикум: нормативно-правовой ландшафт	Пр	0/-/-
АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	Разработка модели угроз для кредитной организации	Пр	0/-/-
АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	Анализ типовых уязвимостей и практика пентеста	Пр	0/-/-
АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ	Практикум по криптографической защите	Пр	0/-/-

ОРГАНИЗАЦИЙ			
УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	Разработка политик информационной безопасности	Пр	2/2/2
УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	Управление инцидентами: от обнаружения до восстановления	Пр	2/-/2
УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	Итоговый практикум: комплексный аудит кибербезопасности организации	Пр	2/-/2
Итого			

5.3. Курсовой проект (работа) учебным планом не предусмотрен

5.4. Самостоятельная работа обучающегося

Темы и/или виды самостоятельной работы	Часы
Самостоятельное изучение лекционного материала и подготовка к практическому занятию	18
Самостоятельное изучение лекционного материала и подготовка к практическому занятию	40
Самостоятельное изучение материала и подготовка к практическим занятиям	36

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

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Кибербезопасность в финансовой системе» размещено в электронной информационно -образовательной сре-де Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Кибербезопасность в финансовой системе».

2.Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Кибербезопасность в финансовой системе».

3. Методические рекомендации по выполнению письменных работ () (при наличии).

4. Методические рекомендации по выполнению контрольной работы студентами заочной формы обучения (при наличии)

5. Методические указания по выполнению курсовой работы (проекта) (при наличии).

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)		
		основная (из п.8 РПД)	дополнительная (из п.8 РПД)	метод. лит. (из п.8 РПД)
1	ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ФИНАНСОВОЙ СФЕРЕ. Самостоятельное изучение лекционного материала и подготовка к практическому занятию	Л1.1, Л1.2	Л2.1, Л2.2, Л2.3	Л3.1
2	АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Самостоятельное изучение лекционного материала и подготовка к практическому занятию	Л1.1, Л1.2	Л2.1, Л2.2, Л2.3	Л3.1
3	УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ. Самостоятельное изучение материала и подготовка к практическим занятиям	Л1.1, Л1.2	Л2.1, Л2.2, Л2.3	Л3.1

7. Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине «Кибербезопасность в финансовой системе»

7.1. Перечень индикаторов компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетен-ции	

7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Кибербезопасность в финансовой системе» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения

обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её корректировке, а также для совершенствования методики обучения, организации учебной работы и оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Кибербезопасность в финансовой системе» проводится в виде Зачет.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО». (или «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО» для дифференцированного зачета/экзамена)

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретиче-ских и практических знаний и навыков студентов по дисциплине.

Состав балльно-рейтинговой оценки студентов очной формы обучения

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций	Максимальное количество баллов
2 курс		
КТ 1	Тест	15
КТ 2	Тест	15
Сумма баллов по итогам текущего контроля		**30**
Посещение лекционных занятий		20
Посещение практических/лабораторных занятий		20
Результативность работы на практических/лабораторных занятиях		30
Итого		100

№ контрольной точки	Оценочное средство результатов индикаторов достижений компетенций	Максимальное количество баллов	Критерии оценки знаний студентов
2 курс			
КТ 1	Тест	15	11-15 баллов выставляется обучающемуся, если тестовые задания выполняются на 85% и выше; 8-10 баллов выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%; 5-7 баллов выставляется обучающемуся, если тестовые задания выполняются на 55 – 69 %; 1-4 балла выставляется обучающемуся, если тестовые задания выполняются на 45 – 54%; 0 баллов выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

КТ 2	Тест	15	11-15 баллов выставляется обучающемуся, если тестовые задания выполняются на 85% и выше; 8-10 баллов выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%; 5-7 баллов выставляется обучающемуся, если тестовые задания выполняются на 55 – 69 %; 1-4 балла выставляется обучающемуся, если тестовые задания выполняются на 45 – 54%; 0 баллов выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

Критерии и шкалы оценивания результатов обучения на промежуточной аттестации

При проведении итоговой аттестации «зачет» («дифференцированный зачет», «экзамен») преподавателю с согласия студента разрешается выставлять оценки («отлично», «хорошо», «удовлетворительно», «зачет») по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет (дифференцированный зачет, экзамен) по приведенным выше вопросам и заданиям. Итоговая успеваемость (зачет, дифференцированный зачет, экзамен) не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче (зачета, дифференцированного зачета, экзамена) к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на (зачете, дифференцированном зачете, экзамене) и сумма баллов переводится в оценку.

Критерии и шкалы оценивания ответа на зачете

По дисциплине «Кибербезопасность в финансовой системе» к зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и без привязке к набранным баллам. Студентам, набравшим более 65 баллов, зачет выставляется по результатам текущей успеваемости, студенты, не набравшие 65 баллов, сдают зачет по вопросам, предусмотренным РПД. Максимальная сумма баллов по промежуточной аттестации (зачету) устанавливается в 15 баллов

Вопрос билета	Количество баллов
Теоретический вопрос	до 5
Задания на проверку умений	до 5
Задания на проверку навыков	до 5

Теоретический вопрос

5 баллов выставляется студенту, полностью освоившему материал дисциплины или курса в соответствии с учебной программой, включая вопросы рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по экзаменационному заданию (билету) и дополнительным вопросам, заданных экзаменатором. Дополнительные вопросы, как правило, должны относиться к материалу дисциплины или курса, не отраженному в основном экзаменационном задании (билете) и выявляют полноту знаний студента по дисциплине.

4 балла заслуживает студент, ответивший полностью и без ошибок на вопросы экзаменационного задания и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

3 балла дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и

несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

2 балла дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

1 балл дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов - при полном отсутствии ответа, имеющего отношение к вопросу.

Задания на проверку умений и навыков

5 баллов Задания выполнены в обозначенный преподавателем срок, письменный отчет без замечаний. Работа выполнена в полном объеме с соблюдением необходимой последовательности.

4 балла Задания выполнены в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.

2 баллов Задания выполнены с задержкой, письменный отчет с недочетами. Работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

1 баллов Задания выполнены частично, с большим количеством вычислительных ошибок, объем выполненной части работы не позволяет сделать правильных выводов.

0 баллов Задания выполнены, письменный отчет не представлен или работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов.

7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Кибербезопасность в финансовой системе»

Раздел 1. Основы кибербезопасности и нормативно-правовое регулирование

1. Выберите один правильный ответ:

Какой нормативный документ устанавливает базовый состав организационных и технических мер защиты информации в финансовых организациях в РФ?

А) ФЗ-149 «Об информации, информационных технологиях и о защите информации»

Б) ГОСТ Р 57580.1-2017

В) PCI DSS

Г) ISO/IEC 27001

Правильный ответ: Б

2. Выберите один правильный ответ:

Кто является основным регулятором в области обеспечения кибербезопасности кредитно-финансовой системы Российской Федерации?

А) Министерство цифрового развития

Б) ФСТЭК России

В) Банк России

Г) Роскомнадзор

Правильный ответ: В

3. Выберите несколько правильных ответов:

Какие из перечисленных органов власти осуществляют нормативно-правовое регулирование в сфере защиты информации в финансовой системе РФ?

А) Банк России

Б) Федеральная служба безопасности (ФСБ)

В) Министерство финансов

Г) Федеральная служба по техническому и экспортному контролю (ФСТЭК)

Правильные ответы: А, Б, Г

Раздел 2. Архитектура угроз и методы защиты
4. Выберите один правильный ответ:

Какой тип атак заключается во взломе интернет-банка через уязвимости в стороннем программном обеспечении, используемом для расчетов?

А) Атака на цепочку поставок

Б) Фишинг

В) DDoS-атака

Г) MITM (атака «человек посередине»)

Правильный ответ: А

5. Выберите один правильный ответ:

Какая система предназначена для сбора, корреляции и анализа событий безопасности в реальном времени?

А) DLP

Б) SIEM

В) IDS

Г) VPN

Правильный ответ: Б

6. Установите соответствие:

Вид угрозы Пример реализации

1. Внутренний нарушитель А) DDoS-атака на сайт банка

2. Внешний злоумышленник Б) Умышленные действия сотрудника с целью кражи баз клиентов

3. Техногенная угроза В) Сбой электропитания дата-центра

Правильные ответы: 1-Б, 2-А, 3-В.

Раздел 3. Управление киберустойчивостью

7. Выберите один правильный ответ:

Какой документ должен быть разработан в финансовой организации для регламентации действий сотрудников при обнаружении признаков компрометации информации?

А) Политика конфиденциальности

Б) План реагирования на инциденты (IRP)

В) Должностная инструкция системного администратора

Г) Стратегия цифровой трансформации

Правильный ответ: Б

8. Выберите один правильный ответ:

Что из перечисленного относится к этапу «Сдерживание» (Containment) в рамках реагирования на инцидент ИБ?

А) Изменение паролей и отключение зараженного сегмента сети

Б) Уведомление регулятора

В) Проведение расследования причин

Г) Публичные комментарии в СМИ

Правильный ответ: А

2. СИТУАЦИОННЫЕ ЗАДАЧИ (КЕЙСЫ) ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Кейс 1 (к Практическому занятию №2, раздел 1)

Ситуация: В коммерческом банке «Альфа-Финанс» произошла утечка персональных данных клиентов (ФИО, номера телефонов, адреса электронной почты). Внутреннее расследование установило, что инцидент произошел из-за заражения рабочей станции сотрудника отдела маркетинг вирусом-стилером. Сотрудник открыл вредоносное вложение в фишинговом письме, пришедшем на корпоративную почту.

Задания:

Определите, какие требования регулятора (Банк России, 152-ФЗ) были нарушены.

Предложите срочные меры по локализации и устранению последствий инцидента.

Разработайте план профилактических мероприятий (технических и организационных) для предотвращения подобных инцидентов в будущем.

Оцените риски репутационных и финансовых потерь для банка.

Кейс 2 (к Практическому занятию №6, раздел 3)

Ситуация: В банке «Гамма» система мониторинга (SIEM) зафиксировала множественные неудачные попытки входа в АБС (автоматизированную банковскую систему) в нерабочее время с нестандартных IP-адресов. Через 15 минут служба безопасности обнаружила, что одна учетная запись операциониста была скомпрометирована, и с нее были отправлены три распоряжения на перевод крупных денежных сумм на счета в иностранных банках.

Задания:

Опишите пошаговый алгоритм действий команды реагирования на инцидент (CERT/CSIRT) в первые 30 минут.

Составьте временную шкалу (timeline) инцидента.

Подготовьте черновик уведомления в Банк России по форме 508-ФЗ (об инциденте).

Предложите изменения в настройки политик доступа и правила контроля операций, чтобы минимизировать риск повторения ситуации.

Кейс 3 (к Практическому занятию №7, раздел 3)

Ситуация: В ходе планового аудита ИБ в банке «Дельта» аудиторы выявили следующие нарушения:

Отсутствует актуальная модель угроз.

Пароли сотрудников не соответствуют требованиям сложности (встречаются даты рождения).

Система резервного копирования не тестируется на восстановление (RPO и RTO не актуальны).

Отсутствует регламент взаимодействия с регулятором при компрометации ключей ЭП.

Задания:

Оцените критичность каждого выявленного нарушения по 5-балльной шкале с обоснованием.

Составьте план мероприятий по устранению нарушений с указанием сроков и ответственных.

Подготовьте аудиторское заключение (выводы и рекомендации) для руководства банка.

3. ПРАКТИЧЕСКИЕ РАСЧЕТНЫЕ ЗАДАНИЯ

Задание 1. Оценка риска

Условие: Вероятность реализации угрозы «Компрометация сервера баз данных» в банке составляет 5% в год. Ожидаемый ущерб (включая штрафы, упущенную выгоду и затраты на восстановление) оценивается в 50 млн рублей. Стоимость внедрения новой системы защиты (WAF + мониторинг) составляет 3 млн рублей единовременно и 1 млн рублей ежегодно на поддержку.

Вопрос: Целесообразно ли внедрять данную систему защиты с точки зрения управления рисками? Рассчитайте показатель ROI для защитных мер.

Решение (примерное):

Годовой ожидаемый ущерб до внедрения: 50 млн * 0,05 = 2,5 млн руб.

Затраты на защиту в первый год: 3 + 1 = 4 млн руб.

Предположим, что система снижает вероятность реализации угрозы на 80% (до 1%).

Остаточный годовой ущерб: 50 млн * 0,01 = 0,5 млн руб.

Снижение ущерба: 2,5 - 0,5 = 2,0 млн руб.

Вывод: в первый год затраты превышают выгоду (4 млн > 2 млн), однако во второй год и далее затраты составят 1 млн руб., а выгода — 2 млн руб., что делает меру экономически целесообразной в долгосрочной перспективе.

Задание 2. Расчет стойкости криптографической защиты

Условие: Для защиты каналов передачи данных в банке используется симметричный алгоритм с длиной ключа 128 бит. Злоумышленник имеет вычислительную мощность, позволяющую перебирать 10^15 ключей в секунду.

Вопрос: Рассчитайте время, необходимое для полного перебора всех ключей (в годах). Оцените, является ли данная защита стойкой на ближайшие 10 лет.

Решение:

Общее количество ключей: 2^128 ≈ 3,4 * 10^38.

Время в секундах: (3,4 * 10^38) / (10^15) = 3,4 * 10^23 секунд.

Время в годах: (3,4 * 10^23) / (60 * 60 * 24 * 365) ≈ 1,08 * 10^16 лет.

Вывод: даже при такой мощности подбор ключа займет миллиарды миллиардов лет, что обеспечивает высокую стойкость.

Темы письменных работ охватывают ключевые вопросы по направлению «кибербезопасность в финансовой системе» и предполагают самостоятельный анализ и решение прикладных задач.

Анализ целевых кибератак (APT) на финансовый сектор РФ в 2024–2026 гг.

Криптовалюты и цифровой рубль: новые угрозы для финансовой стабильности.

Применение дипфейков для мошенничества в системах дистанционного банковского обслуживания (ДБО).

Постквантовая криптография: вызовы и решения для банковской индустрии.

Правовые аспекты и практика обмена данными о киберинцидентах между финансовыми организациями (киберразведка).

Импортозамещение в сфере ИБ: переход на российское ПО в банках.

Методология построения Security Operations Center (SOC) в крупном банке.

Раздел 1. Основы кибербезопасности и нормативно-правовое регулирование

1. Выберите один правильный ответ:

Какой нормативный документ устанавливает базовый состав организационных и технических мер защиты информации в финансовых организациях в РФ?

А) ФЗ-149 «Об информации, информационных технологиях и о защите информации»

Б) ГОСТ Р 57580.1-2017

В) PCI DSS

Г) ISO/IEC 27001

Правильный ответ: Б

2. Выберите один правильный ответ:

Кто является основным регулятором в области обеспечения кибербезопасности кредитно-финансовой системы Российской Федерации?

А) Министерство цифрового развития

Б) ФСТЭК России

В) Банк России

Г) Роскомнадзор

Правильный ответ: В

3. Выберите несколько правильных ответов:

Какие из перечисленных органов власти осуществляют нормативно-правовое регулирование в сфере защиты информации в финансовой системе РФ?

А) Банк России

Б) Федеральная служба безопасности (ФСБ)

В) Министерство финансов

Г) Федеральная служба по техническому и экспортному контролю (ФСТЭК)

Правильные ответы: А, Б, Г

Раздел 2. Архитектура угроз и методы защиты
4. Выберите один правильный ответ:

Какой тип атак заключается во взломе интернет-банка через уязвимости в стороннем программном обеспечении, используемом для расчетов?

А) Атака на цепочку поставок

Б) Фишинг

В) DDoS-атака

Г) MITM (атака «человек посередине»)

Правильный ответ: А

5. Выберите один правильный ответ:

Какая система предназначена для сбора, корреляции и анализа событий безопасности в реальном времени?

А) DLP

Б) SIEM

В) IDS

Г) VPN

Правильный ответ: Б

6. Установите соответствие:

Вид угрозы Пример реализации
1. Внутренний нарушитель А) DDoS-атака на сайт банка
2. Внешний злоумышленник Б) Умышленные действия сотрудника с целью кражи баз клиентов
3. Техногенная угроза В) Сбой электропитания дата-центра
Правильные ответы: 1-Б, 2-А, 3-В.

Раздел 3. Управление киберустойчивостью
7. Выберите один правильный ответ:

Какой документ должен быть разработан в финансовой организации для регламентации действий сотрудников при обнаружении признаков компрометации информации?

А) Политика конфиденциальности

Б) План реагирования на инциденты (IRP)

В) Должностная инструкция системного администратора

Г) Стратегия цифровой трансформации

Правильный ответ: Б

8. Выберите один правильный ответ:

Что из перечисленного относится к этапу «Сдерживание» (Containment) в рамках реагирования на инцидент ИБ?

А) Изменение паролей и отключение зараженного сегмента сети

Б) Уведомление регулятора

В) Проведение расследования причин

Г) Публичные комментарии в СМИ

Правильный ответ: А

2. СИТУАЦИОННЫЕ ЗАДАЧИ (КЕЙСЫ) ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ
Кейс 1 (к Практическому занятию №2, раздел 1)
Ситуация: В коммерческом банке «Альфа-Финанс» произошла утечка персональных данных клиентов (ФИО, номера телефонов, адреса электронной почты). Внутреннее расследование установило, что инцидент произошел из-за заражения рабочей станции сотрудника отдела маркетинг вирусом-стилером. Сотрудник открыл вредоносное вложение в фишинговом

письме, пришедшем на корпоративную почту.

Задания:

Определите, какие требования регулятора (Банк России, 152-ФЗ) были нарушены.

Предложите срочные меры по локализации и устранению последствий инцидента.

Разработайте план профилактических мероприятий (технических и организационных) для предотвращения подобных инцидентов в будущем.

Оцените риски репутационных и финансовых потерь для банка.

Кейс 2 (к Практическому занятию №6, раздел 3)

Ситуация: В банке «Гамма» система мониторинга (SIEM) зафиксировала множественные неудачные попытки входа в АБС (автоматизированную банковскую систему) в нерабочее время с нестандартных IP-адресов. Через 15 минут служба безопасности обнаружила, что одна учетная запись операциониста была скомпрометирована, и с нее были отправлены три распоряжения на перевод крупных денежных сумм на счета в иностранных банках.

Задания:

Опишите пошаговый алгоритм действий команды реагирования на инцидент (CERT/CSIRT) в первые 30 минут.

Составьте временную шкалу (timeline) инцидента.

Подготовьте черновик уведомления в Банк России по форме 508-ФЗ (об инциденте).

Предложите изменения в настройки политик доступа и правила контроля операций, чтобы минимизировать риск повторения ситуации.

Кейс 3 (к Практическому занятию №7, раздел 3)

Ситуация: В ходе планового аудита ИБ в банке «Дельта» аудиторы выявили следующие нарушения:

Отсутствует актуальная модель угроз.

Пароли сотрудников не соответствуют требованиям сложности (встречаются даты рождения).

Система резервного копирования не тестируется на восстановление (RPO и RTO не актуальны).

Отсутствует регламент взаимодействия с регулятором при компрометации ключей ЭП.

Задания:

Оцените критичность каждого выявленного нарушения по 5-балльной шкале с обоснованием.

Составьте план мероприятий по устранению нарушений с указанием сроков и ответственных.

Подготовьте аудиторское заключение (выводы и рекомендации) для руководства банка.

3. ПРАКТИЧЕСКИЕ РАСЧЕТНЫЕ ЗАДАНИЯ

Задание 1. Оценка риска

Условие: Вероятность реализации угрозы «Компрометация сервера баз данных» в банке составляет 5% в год. Ожидаемый ущерб (включая штрафы, упущенную выгоду и затраты на восстановление) оценивается в 50 млн рублей. Стоимость внедрения новой системы защиты (WAF + мониторинг) составляет 3 млн рублей единовременно и 1 млн рублей ежегодно на поддержку.

Вопрос: Целесообразно ли внедрять данную систему защиты с точки зрения управления рисками? Рассчитайте показатель ROI для защитных мер.

Решение (примерное):

Годовой ожидаемый ущерб до внедрения: 50 млн * 0,05 = 2,5 млн руб.

Затраты на защиту в первый год: 3 + 1 = 4 млн руб.

Предположим, что система снижает вероятность реализации угрозы на 80% (до 1%).

Остаточный годовой ущерб: 50 млн * 0,01 = 0,5 млн руб.

Снижение ущерба: 2,5 - 0,5 = 2,0 млн руб.

Вывод: в первый год затраты превышают выгоду (4 млн > 2 млн), однако во второй год и далее затраты составят 1 млн руб., а выгода — 2 млн руб., что делает меру экономически целесообразной в долгосрочной перспективе.

Задание 2. Расчет стойкости криптографической защиты

Условие: Для защиты каналов передачи данных в банке используется симметричный алгоритм с длиной ключа 128 бит. Злоумышленник имеет вычислительную мощность, позволяющую перебирать 10^15 ключей в секунду.

Вопрос: Рассчитайте время, необходимое для полного перебора всех ключей (в годах). Оцените, является ли данная защита стойкой на ближайшие 10 лет.

Решение:

Общее количество ключей: 2^128 ≈ 3,4 * 10^38.

Время в секундах: (3,4 * 10^38) / (10^15) = 3,4 * 10^23 секунд.

Время в годах: (3,4 * 10^23) / (60 * 60 * 24 * 365) ≈ 1,08 * 10^16 лет.

Вывод: даже при такой мощности подбор ключа займет миллиарды миллиардов лет, что обеспечивает высокую стойкость.

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

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

основная

Л1.1 Баланов А. Н. Защита информационных систем. Кибербезопасность [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат. - Санкт-Петербург: Лань, 2024. - 280 с. – Режим доступа: https://e.lanbook.com/book/394544

Л1.2 Козачок А. В. Технологии машинного обучения в кибербезопасности [Электронный ресурс]:учеб. пособие; ВО - Магистратура. - Москва: РТУ МИРЭА, 2024. - 106 с. – Режим доступа: https://e.lanbook.com/book/420881

дополнительная

Л2.1 Гришина Н. В. Информационная безопасность предприятия [Электронный ресурс]:Учебное пособие; ВО - Бакалавриат. - Москва: Издательство "ФОРУМ", 2016. - 239 с. – Режим доступа: http://new.znanium.com/go.php?id=544554

Л2.2 Ковалев Д. В., Богданова Е. А. Информационная безопасность [Электронный ресурс]:учеб. пособие; ВО - Магистратура. - Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016. - 74 с. – Режим доступа: http://new.znanium.com/go.php?id=997105

Л2.3 Борисов С. А., Волкова Е. С., Гисин В. Б., Дворянкин С. В., Козьминых С. И., Королев В.И., Ларионова С.Л., Велигура А.Н., Слезнев В.М., Прокушев Я.Е., Шумилов Ю.Ю., Козьминых С.И. Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики [Электронный ресурс]:моногр. ; ВО - Бакалавриат. - Москва: КноРус, 2021. - 281 с. – Режим доступа: https://book.ru/book/941548

б) Методические материалы, разработанные преподавателями кафедры по дисциплине, в соответствии с профилем ОП.

Л3.1 Биткина И. К. Экономическая безопасность финансового рынка [Электронный ресурс]:учеб. пособие ; ВО - Бакалавриат. - Москва: Русайнс, 2024. - 154 с. – Режим доступа: https://book.ru/book/953623

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

№	Наименование ресурса сети «Интернет»	Электронный адрес ресурса
1	Электронно-библиотечная система «Znanium». — Текст: электронный. — URL: https://znanium.com (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей.	https://znanium.com
2	Электронно-библиотечная система «Лань». — Текст: электронный. — URL: https://e.lanbook.com (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей.	https://e.lanbook.com
3	Образовательная платформа «Юрайт». — Текст: электронный. — URL: https://urait.ru (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей.	https://urait.ru

10. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины предполагает последовательное изучение теоретического материала и закрепление практических навыков по направлению «кибербезопасность в финансовой системе» на практических (лабораторных) занятиях. Рекомендуется систематическая работа в течение семестра, своевременное выполнение заданий и подготовка к контрольным точкам.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).

11.1 Перечень лицензионного программного обеспечения

1. Kaspersky Endpoint Security 12.11 - Антивирус
2. Microsoft Windows Server STDCORE AllLngLicense/Software AssurancePack Academic OLV 16Licenses LevelE AdditionalProduct CoreLic 1Year - Серверная операционная система

11.3 Перечень программного обеспечения отечественного производства

1. Kaspersky Endpoint Security 12.11 - Антивирус

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

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

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Номер аудитории	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Учебная аудитория для проведения занятий всех типов (в т.ч. лекционного, семинарского, практической подготовки обучающихся), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	315/НК	Оснащение: специализированная мебель на 250 посадочных мест, трибуна для лектора – 1 шт., президиум – 1 шт., видеостена из 9 бесшовный ЖК дисплеев Mercury Full HD 55” ширина-3,1 м высота - 1,7 м , АРМ на основе Intel Core i3 , Монитор Dell 21.5", Клавиатура + мышь , Источник бесперебойного питания 650ВА, Монитор ЖК размер экрана: Dell 21.5", широкоформатная матрица VA с разрешением 1920×1080, отношением сторон 16:9 - 3шт.,микрофонная система Restmoment RX-812 -1шт, Restmoment RX-D58 микрофон делегата -4шт.,АМС настенный громкоговоритель мониторного типа - 6шт., DSPPA микшер-усилитель - 1шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
		423/НК	Оснащение: специализированная мебель на 56 посадочных мест, стол преподавателя – 1 шт., Sharp 70" Информационный ЖК-дисплей – 1 шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
2	Помещение для самостоятельной работы обучающихся, подтверждающее наличие материально-технического обеспечения, с перечнем основного оборудования		

		214/НК библиотека	Специализированная мебель на 130 посадочных мест, персональные компьютеры, моноблоки – 80 шт., копир А3 - 3, принтер матричный - 2, МФУ ч/б – 7 шт., МФУ цветной – 2 шт., принтер ч/б – 8 шт., принтер цветн. - 2 шт., сканер – 2 шт., сканеры штрих-кода - 5, наушники - 10 шт., Wi-Fi оборудование, подключение к сети «Интернет», доступ к российским и международным ресурсам и базам данных, доступ к электронно-библиотечным системам, доступ в электронную информационно-образовательную среду университета. Открытый доступ к фонду учебной, научной и художественной литературы.

13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Кибербезопасность в финансовой системе» составлена на основе Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 38.04.01 Экономика (приказ Минобрнауки России от 11.08.2020 г. № 939).

Автор (ы)

_____ доц. КИС, ктн Березницкий Андрей Сергеевич

Рецензенты

_____ доц. КИС, ктн Трошков Александр Михайлович

_____ проф. КИС, дэн Шуваев Алксандр Васильевич

Рабочая программа дисциплины «Кибербезопасность в финансовой системе» рассмотрена на заседании Кафедра информационных систем протокол № 9 от 07.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 38.04.01 Экономика

Заведующий кафедрой _____ Березницкий Андрей Сергеевич

Рабочая программа дисциплины «Кибербезопасность в финансовой системе» рассмотрена на заседании учебно-методической комиссии Институт экономики, финансов и управления в АПК протокол № 2 от 08.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 38.04.01 Экономика

Руководитель ОП _____