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.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

Б1.В.03 Кибербезопасность в финансовой системе

38.04.01 Экономика

Финансовый контроль и цифровизация экономической деятельности

магистр

заочная

Ставрополь, 2026

1. 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	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.

2. Перечень оценочных средств по дисциплине

№	Наименование раздела/темы	Курс	Код индикаторов достижения компетенций	Оценочное средство проверки результатов достижения индикаторов компетенций
1.	1 раздел. Раздел 1			
1.1.	ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ФИНАНСОВОЙ СФЕРЕ	2	ПК-2.2	Тест
1.2.	АРХИТЕКТУРА УГРОЗ И МЕТОДЫ ЗАЩИТЫ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	2	ПК-2.2	Устный опрос
1.3.	УПРАВЛЕНИЕ КИБЕРУСТОЙЧИВОСТЬЮ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ	2	ПК-2.2	Тест
	Промежуточная аттестация			За

3. Оценочные средства (оценочные материалы)

Примерный перечень оценочных средств для текущего контроля успеваемости и промежуточной аттестации

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде (Оценочные материалы)
Текущий контроль			

	Для оценки знаний		
1	Устный опрос	Средство контроля знаний студентов, способствующее установлению непосредственного контакта между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала.	Перечень вопросов для устного опроса
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
	Для оценки умений		
	Для оценки навыков		
	Промежуточная аттестация		
3	Зачет	Средство контроля усвоения учебного материала практических и семинарских занятий, успешного прохождения практик и выполнения в процессе этих практик всех учебных поручений в соответствии с утвержденной программой с выставлением оценки в виде «зачтено», «незачтено».	Перечень вопросов к зачету

4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Кибербезопасность в финансовой системе"

Примерные оценочные материалы для текущего контроля успеваемости

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.

Примерные оценочные материалы
для проведения промежуточной аттестации (зачет, экзамен)
по итогам освоения дисциплины (модуля)

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 (эссе, рефераты, курсовые работы и др.)

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.