Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Т.К. Платонова
«25» мая 2026 г.

Рабочая программа дисциплины
Кибербезопасность в банковском бизнесе и цифровых экосистемах

Направление подготовки
38.04.08 Финансы и кредит

Направленность (профиль) программы магистратуры
38.04.08.06 Финтех в банковском бизнесе и цифровых экосистемах

Для набора 2026 года

Квалификация
магистр

КАФЕДРА **Банковское дело**

Распределение часов дисциплины по семестрам / курсам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	6	6	6	6
Практические	14	14	14	14
Итого ауд.	20	20	20	20
Контактная работа	20	20	20	20
Сам. работа	52	52	52	52
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом Университета (протокол № 9 от 03.03.2026 г.).

Программу составил(и): д.э.н., профессор, Добролежа Е.В.

Зав. кафедрой: д.э.н., профессор О.Г. Семенюта

Методический совет направления: д.э.н., профессор О.Б. Иванова

Директор института магистратуры: д.э.н., профессор Е.А. Иванова

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	применение на основе анализа киберугроз приёмов и методов, повышающих уровень кибербезопасности в банковском бизнесе и цифровых экосистемах

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3. Способен формировать требования к системе платежных сервисов и инструментов

В результате освоения дисциплины обучающийся должен:

Знать:

методологические подходы к информационной безопасности и киберустойчивости субъектов банковского бизнеса и цифровых экосистем,
принципы применения методов защиты, а также типологии киберугроз и киберпространства (соотнесение с индикатором ПК-3.1)

Уметь:

применять нормативные требования в сфере информационной безопасности, выявлять угрозы и проводить анализ информации для принятия решений по обеспечению информационной безопасности в банках и цифровых экосистемах (соотнесение с индикатором ПК-3.2)

Владеть:

разработки рекомендаций по обеспечению информационной безопасности на всех этапах жизненного цикла платёжных сервисов и инструментов с учётом особенностей реализации технологий защиты и развития новых подходов к обеспечению кибербезопасности (соотнесение с индикатором ПК-3.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы кибербезопасности в банковском секторе и цифровых экосистемах

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема 1.1. «Основы кибербезопасности и киберпреступности в банковском бизнесе и цифровых экосистемах» Понятие кибербезопасности, кибертерроризма и киберпреступности. Нормативно-правовое регулирование кибербезопасности в банковском бизнесе и цифровых экосистемах. Механизм распределения полномочий в сфере защиты от киберпреступлений и кибератак в банковском секторе и цифровых экосистемах. Стандарты кибербезопасности. Тема 1.2. «Киберпреступления и методы защиты» Классификация типов киберпреступлений. Классификация киберпреступников и методы их действий. Способы защиты от киберпреступлений. Противодействие легализации бизнеса по разработке шпионских программ.	Лекционные занятия	2	2	ПК-3
1.2	Тема 1.1. «Основы кибербезопасности и киберпреступности в банковском бизнесе и цифровых экосистемах» Понятие кибербезопасности, кибертерроризма и киберпреступности. Нормативно-правовое регулирование кибербезопасности в банковском бизнесе и цифровых экосистемах. Механизм распределения полномочий в сфере защиты от киберпреступлений и кибератак в банковском секторе и цифровых экосистемах. Стандарты кибербезопасности. Выполнение ситуационных заданий, аналитических заданий, комплексных заданий.	Практические занятия	2	2	ПК-3
1.3	Тема 1.2. «Киберпреступления и методы защиты» Классификация типов киберпреступлений. Классификация киберпреступников и методы их действий. Способы защиты от киберпреступлений. Противодействие легализации бизнеса по разработке шпионских программ. Выполнение ситуационных заданий, аналитических заданий, комплексных заданий.	Практические занятия	2	4	ПК-3
1.4	Тема 1.1. «Основы кибербезопасности и киберпреступности в банковском бизнесе и цифровых экосистемах»	Самостоятельная работа	2	12	ПК-3

	Понятие кибербезопасности, кибертерроризма и киберпреступности. Нормативно-правовое регулирование кибербезопасности в банковском бизнесе и цифровых экосистемах. Механизм распределения полномочий в сфере защиты от киберпреступлений и кибератак в банковском секторе и цифровых экосистемах. Стандарты кибербезопасности. Подготовка ситуационных заданий, аналитических заданий, комплексных заданий. Подготовка к прохождению тестов.				
1.5	Тема 1.2. «Киберпреступления и методы защиты» Классификация типов киберпреступлений. Классификация киберпреступников и методы их действий. Способы защиты от киберпреступлений. Легализация бизнеса по разработке шпионских программ. Подготовка ситуационных заданий, аналитических заданий, комплексных заданий. Подготовка к прохождению тестов.	Самостоятельная работа	2	12	ПК-3

Раздел 2. Кибербезопасность в условиях цифровой трансформации

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	Тема 2.1. «Кибероружие и кибервойны на финансовом рынке» Краткая история развития кибероружия. Методологические принципы классификации кибероружия. Проблемы идентификации исполнителей и заказчиков кибератак.	Лекционные занятия	2	2	ПК-3
2.2	Тема 2.2. «Технологии и методы обеспечения кибербезопасности на финансовом рынке» Типовые уязвимости в системах киберзащиты. Методы выявления программных уязвимостей. Антивирусные программы и иммунный подход к защите. Кибер разведка, киберконтрразведка и обеспечение кибербезопасности.	Лекционные занятия	2	2	ПК-3
2.3	Тема 2.1. «Кибероружие и кибервойны на финансовом рынке» Краткая история развития кибероружия. Методологические принципы классификации кибероружия. Проблемы идентификации исполнителей и заказчиков кибератак. Выполнение ситуационных заданий, аналитических заданий, комплексных заданий.	Практические занятия	2	4	ПК-3
2.4	Тема 2.2. «Технологии и методы обеспечения кибербезопасности на финансовом рынке» Типовые уязвимости в системах киберзащиты. Методы выявления программных уязвимостей. Антивирусные программы и иммунный подход к защите. Кибер разведка, киберконтрразведка и обеспечение кибербезопасности. Выполнение ситуационных заданий, аналитических заданий, комплексных заданий.	Практические занятия	2	4	ПК-3
2.5	Тема 2.1. «Кибероружие и кибервойны на финансовом рынке» Краткая история развития кибероружия. Методологические принципы классификации кибероружия. Проблемы идентификации исполнителей и заказчиков кибератак. Подготовка ситуационных заданий, аналитических заданий, комплексных заданий. Подготовка к прохождению тестов.	Самостоятельная работа	2	12	ПК-3
2.6	Тема 2.2. «Технологии и методы обеспечения кибербезопасности на финансовом рынке» Типовые уязвимости в системах киберзащиты. Методы выявления программных уязвимостей. Антивирусные программы и иммунный подход к защите. Кибер разведка, киберконтрразведка и обеспечение кибербезопасности. Подготовка ситуационных заданий, аналитических заданий, комплексных заданий. Подготовка к прохождению тестов.	Самостоятельная работа	2	16	ПК-3
2.7	Подготовка к промежуточной аттестации	Зачет	2	0	ПК-3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Белоус, А. И., Солодуха, В. А.	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения	Москва: Техносфера, 2021	ЭБС «IPR SMART»
2		Финансовые исследования	, 2000	ЭБС «IPR SMART»
3	Бердюгин, А. А., Дудка, А. Б., Конявская, С. В., Назаров, И. Г., Неваленный, А. В., Ожеред, И. В., Ошманкевич, К. Р., Персанов, Д. Ю., Пименов, П. А., Ревенков, П. В., Русин, Л. И., Силин, Н. Н., Фролов, Д. Б., Ревенкова, П. В.	Кибербезопасность в условиях электронного банкинга: практическое пособие	Москва: Прометей, 2020	ЭБС «IPR SMART»
4	Бакунова Т. В., Кожевников О. В., Трофимова Е. А., Фоминых М. М.	Информационные технологии в финансово-кредитной сфере: учебное пособие	Екатеринбург: Издательство Уральского университета, 2020	ЭБС «Университетская библиотека онлайн»
5	Беловицкий К. Б., Булатенко М. А., Кузовлева Н. Ф., Микаева А. С.	Экономическая безопасность: учебник для вузов: учебник	Москва: Дашков и К°, 2024	ЭБС «Университетская библиотека онлайн»
6		Финансы и кредит: журнал	Москва: Финансы и кредит, 2024	ЭБС «Университетская библиотека онлайн»
7		Национальные интересы : приоритеты и безопасность: журнал	Москва: Финансы и кредит, 2024	ЭБС «Университетская библиотека онлайн»

5.2. Профессиональные базы данных и информационные справочные системы

ИСС «КонсультантПлюс»
ИСС «Гарант» http://www.internet.garant.ru/
Базы данных Центрального банка РФ https://www.cbr.ru/hd_base/
Базы данных Федеральной службы государственной статистики https://www.gks.ru/databases
Базы данных Ассоциации развития финансовых технологий (Ассоциация ФинТех) https://www.fintechru.org/
База данных СПАРК ИНТЕРФАКС http://www.spark-interfax.ru/system/#/dnb
База данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации https://digital.gov.ru/ru/activity/statistic/
База данных Национальной Ассоциации международной информационной безопасности https://namib.online/
База данных АО «Лаборато́рия Каспе́рского» https://support.kaspersky.com/

5.3. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice.

5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к

сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-3: Способен формировать требования к системе платежных сервисов и инструментов			
З методологические подходы к информационной безопасности и киберустойчивости субъектов банковского бизнеса и цифровых экосистем, принципы применения методов защиты, а также типологии киберугроз и киберпространства	решение тестов выполнение комплексного задания ответы в ходе промежуточной аттестации	верность ответа на тестовые задания; полнота и содержательность ответа соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет полнота и содержательность ответа соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	Вопросы к зачету (1-34), тесты (1-36), комплект комплексного задания (1-10), аналитические задания (1-9), ситуационные задания (1-3)
Уметь применять нормативные требования в сфере информационной безопасности, выявлять угрозы и проводить анализ информации для принятия решений по обеспечению информационной безопасности в банках и цифровых экосистемах	выполнение аналитических заданий, решение ситуационных заданий. ответы в ходе промежуточной аттестации	полнота и содержательность приведенного обзора при выполнении аналитического задания, решение ситуационных заданий в соответствии с материалами лекции и учебной литературы, нормативно-правовой базой, обоснованное логически и правильное с расчетной точки зрения полнота и содержательность ответа соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	Вопросы к зачету (1-34), тесты (1-36), комплект комплексного задания (1-10), аналитические задания (1-9), ситуационные задания (1-3)
В навыками разработки рекомендаций по обеспечению	решение ситуационных заданий.	решение ситуационных заданий в соответствии с материалами лекции и учебной литературы, нормативно-правовой базой,	Вопросы к зачету (1-34), тесты (1-36), комплект

информационной безопасности на всех этапах жизненного цикла платёжных сервисов и инструментов с учётом особенностей реализации технологий защиты и развития новых подходов к обеспечению кибербезопасности	ответы в ходе промежуточной аттестации	обоснованное логически и правильное с расчетной точки зрения полнота и содержательность ответа соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	комплексного задания (1-10), аналитические задания (1-9), ситуационные задания (1-3)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Общее понятие о кибербезопасности. Кибертерроризм и киберпреступность.
2. Нормативно-правовое регулирование кибербезопасности в банковском бизнесе и цифровых экосистемах.
3. Механизм распределения полномочий в сфере защиты от киберпреступлений и кибератак в банковском секторе и цифровых экосистемах.
4. Стандарты кибербезопасности. Классификация типов киберпреступлений.
5. Киберпреступления и киберпреступники: классификация, методы действия и способы защиты.
6. Легализация бизнеса по разработке шпионских программ как новая угроза
7. кибербезопасности.
8. Краткая история развития кибероружия
9. Методологические принципы классификации кибероружия
10. Проблемы идентификации исполнителей и заказчиков кибератак
11. Типовые уязвимости в системах киберзащиты
12. Методы выявления программных уязвимостей
13. Антивирусные программы
14. Проактивная антивирусная защита – функции и возможности
15. Иммунный подход к защите информационных систем
16. Классификация, способы и объекты кибершпионажа
17. Кибербразведка и контрразведка: цели, задачи и методы работы
18. Методологические особенности отбора и подготовки специалистов в области кибербразведки и киберконтрразведки
19. Особенности обеспечения кибербезопасности конечных точек
20. инфраструктурных систем
21. Базовые термины и определения кибербезопасности
22. Редтайминг и блютайминг
23. Охота за угрозами как проактивный метод киберзащиты
24. База знаний MITRE ATT&CK
25. SIEM как важный элемент в архитектуре киберзащиты
26. Магический квадрат Gartner
27. Типовые атаки на организации кредитно-финансовой сферы при корпоративном кредитовании и финансовом консультировании
28. Атаки с применением методов социальной инженерии в отношении сотрудников банка

29. Атаки на системы дистанционного банковского обслуживания, используемые юридическими лицами
30. Атаки на клиентов – физических лиц
31. Атаки на устройства самообслуживания (отмена транзакции)
32. Электронный банкинг и риски недостаточного обеспечения информационной безопасности
33. Кибербезопасность в условиях применения систем электронного банкинга
34. Влияние теневого интернета на безопасность электронного банкинга.

Критерии оценивания:

− «зачтено» (50-100 баллов) выставляется, если изложенный магистрантом материал фактически верен, выявлено наличие глубоких исчерпывающих, либо твердых и достаточно полных знаний в объеме изученной темы, грамотное и логически стройное изложение материала при ответе, при возможном наличии отдельных логических и стилистических погрешностей и ошибок, уверенно исправленных после дополнительных вопросов

- «не зачтено» (0-49 баллов) выставляется, если ответы магистранта не связаны с вопросами, при наличии грубых ошибок в ответе, непонимания сущности излагаемого вопроса, неуверенности и неточности ответов на дополнительные и наводящие вопросы

Тесты

1. Что такое кибербезопасность?
   а) Защита информации от несанкционированного доступа.
   б) Обеспечение безопасности компьютерных систем и сетей.
   в) Все ответы верны.
2. Какие основные угрозы существуют в киберпространстве?
   а) Вредоносные программы.
   б) Фишинг и мошенничество.
   в) Утечка данных.
   г) Всё вышеперечисленное.
3. Что такое шифрование данных?
   а) Процесс преобразования данных в зашифрованный формат.
   б) Метод защиты информации путём её преобразования.
   в) Оба ответа верны.
4. Что такое брандмауэр?
   а) Программа для защиты от вредоносных программ.
   б) Система фильтрации трафика.
   в) Устройство для обеспечения безопасности сети.
5. Что такое антивирусное ПО?
   а) Программное обеспечение для обнаружения и удаления вирусов.
   б) Программа для мониторинга сетевого трафика.
   в) Инструмент для шифрования данных.
6. Какие меры предпринимаются банками для обеспечения кибербезопасности?
   а) Внедрение систем аутентификации и авторизации.
   б) Использование шифрования данных при передаче.
   в) Регулярное обновление программного обеспечения.
   г) Все ответы верны.
7. Что такое DDoS-атака?
   а) Атака на сервер с целью его перегрузки.
   б) Попытка взлома системы через уязвимости.
   в) Кража личных данных пользователей.
8. Как банки защищают свои системы от DDoS-атак?
   а) Использование средств обнаружения атак.
   б) Резервное копирование данных.
   в) Применение технологий балансировки нагрузки.

9. Какие риски связаны с использованием мобильных приложений банков?
   а) Угроза утечки данных.
   б) Возможность фишинга.
   в) Риск потери контроля над приложением.
   г) Все ответы верны.
10. Какие технологии используются для аутентификации в банковских приложениях?
   а) Двухфакторная аутентификация.
   б) Биометрическая аутентификация.
   в) SMS-подтверждение.
   г) Все перечисленные.

11. Что такое киберугроза?
   а) Угроза, исходящая от людей или организаций, стремящихся получить несанкционированный доступ к информации или системам с целью причинения вреда или получения выгоды.
   б) Угроза информационной безопасности, связанная с использованием информационных технологий.
   в) Оба ответа верны.

12. Какие виды киберугроз существуют?
   а) Вредоносные программы, фишинг, мошенничество, утечка данных и др.
   б) Физические угрозы, такие как пожары или стихийные бедствия.
   в) Экономические угрозы, связанные с изменением курсов валют или процентных ставок.

13. Что такое фишинг?
   а) Вид мошенничества, при котором злоумышленники пытаются получить конфиденциальную информацию (например, пароли или номера банковских карт), выдавая себя за доверенное лицо.
   б) Использование вредоносных программ для сбора конфиденциальной информации.
   в) Атака на сервер с целью его перегрузки.

14. Что такое мошенничество с платёжными картами?
   а) Незаконное использование платёжной карты для оплаты товаров или услуг без согласия владельца карты.
   б) Кража личных данных пользователей.
   в) Фишинг с использованием платёжных карт.

15. Что такое социальная инженерия?
   а) Метод манипуляции людьми с целью получения конфиденциальной информации или доступа к системам.
   б) Вид киберугроз, связанных с использованием социальных сетей.
   в) Способ защиты от киберугроз путём создания социальных связей.

16. Что такое вредоносное ПО?
   а) Программа, созданная со злым умыслом или злыми намерениями.
   б) Программа, которая может нанести вред компьютеру или сети.
   в) Всё вышеперечисленное.

17. Что такое DDoS-атака?
   а) Попытка сделать систему недоступной для законных пользователей путём отправки большого количества запросов или трафика.
   б) Атака, направленная на получение конфиденциальной информации о пользователях.
   в) Вид социальной инженерии, связанный с обманом пользователей.

18. Что такое переполнение буфера?
   а) Ошибка в программном обеспечении, которая позволяет злоумышленникам выполнить произвольный код на сервере.
   б) Тип атаки на отказ в обслуживании, направленный на перегрузку сервера запросами.

19. Что такое уязвимость?
    а) Слабое место в системе, которое может быть использовано злоумышленниками для получения несанкционированного доступа.
    б) Недостаток в системе безопасности, который может привести к нарушению её целостности или доступности.
    в) Всё вышеперечисленное.

20. Что такое атака на отказ в обслуживании (DoS)?
    а) Попытка сделать систему недоступной для законных пользователей путём отправки большого количества запросов или трафика.
    б) Атака, направленная на получение конфиденциальной информации о пользователях.
    в) Вид социальной инженерии, связанный с обманом пользователей.

21. Что такое переполнение буфера?
    а) Ошибка в программном обеспечении, которая позволяет злоумышленникам выполнить произвольный код на сервере.
    б) Тип атаки на отказ в обслуживании, направленный на перегрузку сервера запросами.

22. Что такое SQL-инъекция?
    а) Метод внедрения вредоносного кода в систему через уязвимости в коде, обрабатывающем запросы к базе данных.
    б) Уязвимость, связанная с недостаточной проверкой входных данных при выполнении запросов к базе данных.
    в) Оба ответа верны.

23. Что такое XSS-атака?
    а) Внедрение вредоносного кода на веб-страницу с целью выполнения этого кода на компьютере пользователя.
    б) Использование уязвимостей в веб-приложениях для выполнения вредоносных действий на стороне клиента.
    в) Оба ответа верны.

24. Что такое CSRF-атака?
    а) Подделка межсайтовых запросов с целью заставить пользователя выполнить нежелательные действия на сайте.
    б) Вид уязвимости, связанной с недостаточной защитой от подделки запросов.
    в) Оба ответа верны.

25. Что такое MITM-атака?
    а) Атака «человек посередине», при которой злоумышленник перехватывает и изменяет данные, передаваемые между двумя сторонами.
    б) Метод взлома, при котором злоумышленник получает доступ к незащищённому каналу связи и может прослушивать или изменять данные.
    в) Оба ответа верны.

26. Что такое утечка данных?
    а) Непреднамеренное раскрытие конфиденциальной информации.
    б) Несанкционированный доступ к данным.
    в) Оба ответа верны.

27. Что такое кибербезопасность?
    а) Защита информации от несанкционированного доступа.
    б) Обеспечение безопасности компьютерных систем и сетей.
    в) Всё вышеперечисленное.

28. Какие основные угрозы существуют в киберпространстве?
    а) Вредоносные программы.
    б) Фишинг и мошенничество.

в) Утечка данных.
г) Всё вышеперечисленное.

29. Что такое шифрование данных?
    а) Процесс преобразования данных в зашифрованный формат.
    б) Метод защиты информации путём её преобразования.
    в) Оба ответа верны.

30. Что такое брандмауэр?
    а) Программа для защиты от вредоносных программ.
    б) Система фильтрации трафика.
    в) Устройство для обеспечения безопасности сети.

31. Что такое антивирусное ПО?
    а) Программное обеспечение для обнаружения и удаления вирусов.
    б) Программа для мониторинга сетевого трафика.
    в) Инструмент для шифрования данных.

32. Какие меры предпринимаются банками для обеспечения кибербезопасности?
    а) Внедрение систем аутентификации и авторизации.
    б) Использование шифрования данных при передаче.
    в) Регулярное обновление программного обеспечения.
    г) Все ответы верны.

33. Как банки защищают свои системы от DDoS-атак?
    а) Использование средств обнаружения атак.
    б) Резервное копирование данных.
    в) Применение технологий балансировки нагрузки.

34. Какие риски связаны с использованием мобильных приложений банков?
    а) Угроза утечки данных.
    б) Возможность фишинга.
    в) Риск потери контроля над приложением.
    г) Все ответы верны.

35. Какие технологии используются для аутентификации в банковских приложениях?
    а) Двухфакторная аутентификация.
    б) Биометрическая аутентификация.
    в) SMS-подтверждение.
    г) Все перечисленные.

36. Какие методы используют банки для защиты платёжных карт?
    а) Шифрование данных о транзакциях.
    б) Многоуровневая аутентификация.
    в) Мониторинг подозрительной активности.
    г) Все вышеперечисленные.

Критерии оценивания:
Максимум 20 баллов. Вариант содержит 10 заданий.
16-20 баллов выставляется, если обучающийся ответил правильно на 84-100% заданий теста;
13-15 баллов, если обучающийся ответил правильно на 67-83 % заданий;
10-12 баллов, если обучающийся ответил правильно на 50-66% заданий;
0-9 баллов, если обучающийся ответил правильно на 0-49% заданий

Комплект комплексного задания

1. Опишите основные угрозы кибербезопасности в банковском секторе и цифровых экосистемах.
2. Назовите основные методы защиты информации в банковской сфере.

3. Расскажите о мерах по предотвращению утечки конфиденциальной информации в банках.

4. Перечислите основные принципы обеспечения безопасности данных в цифровых экосистемах.

5. Опишите процесс шифрования данных в банковской системе.

6. Расскажите о методах защиты от фишинга и социальной инженерии в банковской сфере.

7. Объясните, как работает система двухфакторной аутентификации в банках.

8. Перечислите основные инструменты для мониторинга и анализа угроз кибербезопасности в банковском секторе.

9. Расскажите о методах борьбы с вредоносным ПО в банковской сфере.

10. Опишите процесс реагирования на инциденты кибербезопасности в банках.

Критерии оценивания:

Максимум 30 баллов. Студент выполняет комплект из 10 заданий.

21-30 баллов выставляется, если студент правильно выполнил задание рукописным текстом с обязательной ссылкой на источники информации, в том числе нормы действующего законодательства; в логических рассуждениях и обосновании выполнении задач нет пробелов и ошибок; (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

11-20 баллов выставляется, если студент правильно выполнил ¾ объема заданий рукописным текстом с обязательной ссылкой на источники информации, в том числе нормы действующего законодательства; в логических рассуждениях и обосновании выполнении задач нет пробелов и ошибок; (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала). Если выполнены все задания, но выводы недостаточно аргументированы; допущена одна ошибка или два-три недочета.

1-10 баллов выставляется, если студент правильно выполнил половину объема заданий рукописным текстом с обязательной ссылкой на источники информации, в том числе нормы действующего законодательства; в логических рассуждениях и обосновании выполнении задач нет пробелов и ошибок; (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала). Если выполнены 3/4 заданий, но выводы недостаточно аргументированы; допущена одна ошибка или два-три недочета.

0 баллов выставляется, если допущены существенные ошибки, показавшие, что обучающийся не владеет обязательными знаниями и навыками; правильно выполнено менее половины работы.

Аналитические задания

1. Проанализируйте основные угрозы и риски кибербезопасности в банковском секторе. Предложите комплекс мер по их предотвращению и минимизации.

2. Раскройте роль и значение стандартов и нормативно-правовых актов в области обеспечения кибербезопасности в банковской деятельности. Приведите примеры ключевых документов.

3. Охарактеризуйте современные технологии и методы защиты информации, применяемые в банковских системах и цифровых экосистемах. Оцените их эффективность.

4. Проведите сравнительный анализ подходов к управлению рисками информационной безопасности в банковском секторе и цифровых экосистемах. Выявите ключевые различия и общие принципы.

5. Раскройте роль и функции подразделений информационной безопасности в банковских организациях. Обоснуйте необходимость их взаимодействия с другими структурными подразделениями.

6. Разработайте план мероприятий по обеспечению кибербезопасности для банка, внедряющего новую цифровую услугу. Определите ключевые этапы, ответственных лиц и необходимые ресурсы.

7. Проведите аудит информационной безопасности в одном из подразделений банка. Сформулируйте рекомендации по устранению выявленных уязвимостей и совершенствованию системы защиты.

8. Смоделируйте сценарий кибератаки на банковскую систему и разработайте план действий по реагированию и ликвидации последствий инцидента. Определите роли и ответственность участников.

9. Разработайте программу обучения и повышения осведомленности сотрудников банка в области кибербезопасности. Обоснуйте ее содержание и формы реализации.

Критерии оценивания:

Максимум 20 баллов. Задания студент выбирает по своему желанию.

16-20 баллов выставляется, если магистрант выполнил 4 аналитических задания, полно и содержательно раскрывая решение выполненных заданий на основе приведенного обзора.

11-15 баллов выставляется, если магистрант выполнил 3 аналитических задания, полно и содержательно раскрывая решение выполненных заданий на основе приведенного обзора.

6-10 баллов выставляется, если магистрант выполнил 2 аналитических задания, полно и содержательно раскрывая решение выполненных заданий на основе приведенного обзора.

1-5 баллов выставляется, если магистрант выполнил 1 аналитическое задание, полно и содержательно раскрывая решение выполненного задания на основе приведенного обзора.

0 баллов выставляется, если магистрант не выполнял задания.

Ситуационные задания

Задание 1. Исследуйте и проанализируйте последние тенденции в области кибербезопасности в банковском секторе и цифровых экосистемах. Подготовьте отчет, включающий анализ угроз, уязвимостей и мер противодействия.

Задание 2. Разработайте план действий по обеспечению кибербезопасности для малого предприятия, работающего в сфере цифровых услуг. План должен включать описание политики безопасности, процедур и технических мер.

Задание 3. Проведите анализ существующих стандартов и рекомендаций по кибербезопасности, таких как ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls и другие. Сравните их и определите, какие из них наиболее применимы для банковского сектора и цифровых экосистем.

Критерии оценивания:

Максимум 30 баллов

21-30 баллов выставляется обучающемуся, если 3 ситуационных задания решены верно и полностью, в соответствии с нормативно-правовой базой; в логических рассуждениях и обосновании решения нет пробелов и ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

11-20 баллов выставляется обучающемуся, если 2 ситуационных задания решены верно и полностью, в соответствии с нормативно-правовой базой; в логических рассуждениях и обосновании решения нет пробелов и ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

0-10 баллов выставляется обучающемуся, если 1 ситуационных задания решены верно и полностью, в соответствии с нормативно-правовой базой; в логических рассуждениях и обосновании решения нет пробелов и ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета

Зачет проводится по расписанию промежуточной аттестации в письменном виде Задание содержит два вопроса. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «КИБЕРБЕЗОПАСНОСТЬ В БАНКОВСКОМ БИЗНЕСЕ И ЦИФРОВЫХ ЭКОСИСТЕМАХ»

Учебным планом предусмотрены следующие виды занятий:

- лекции
- практические занятия.

В ходе лекционных занятий рассматриваются основные вопросы теории организации деятельности банка, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки аналитической работы, принятия управленческих решений.

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников.

Студент должен готовиться к предстоящему практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.

Методические рекомендации по выполнению комплексного задания

Для выполнения задания студент должен:

- изучить теоретический вопрос;
- собрать информацию из открытых источников о практике и возможных путях решения задачи и структурировать ее;
- описать решение задания:
- сделать выводы и представить их в форме доклада или доклада-презентации;
- аргументировать собственную точку зрения по проблеме.

Доклад делается в произвольной форме (приветствуются любые методы изложения материала). Обязательные условия: участие в докладе всех членов группы (приблизительно в равной мере); наличие иллюстративного материала (в любой форме – презентация, раздаточный материал, по смыслу подкрепляющие изложение и делающие его более наглядным и интересным).

По окончании доклада студенты и преподаватель в обязательном порядке задают вопросы. Оценивается качество ответов на вопросы.

Методические рекомендации по выполнению аналитических заданий

Для выполнения аналитических заданий используются данные Росстата, официального сайта ЦБ РФ, Ассоциации ФинТех, Ассоциации цифровых платформ, сайтов кредитных организаций.

Для выполнения задания студент должен:

- изучить теоретический вопрос;
- собрать статистическую информацию и структурировать ее;
- произвести необходимые расчеты и проанализировать собранный материал;
- сделать выводы и представить их в форме доклада или доклада-презентации;
- аргументировать собственную точку зрения по проблеме.

Доклад делается в произвольной форме (приветствуются любые методы изложения материала) с использованием LibreOffice. Обязательные условия: участие в докладе всех членов группы (приблизительно в равной мере); наличие иллюстративного материала (в любой форме – презентация,

раздаточный материал, по смыслу подкрепляющие изложение и делающие его более наглядным и интересным).

По окончании доклада студенты и преподаватель в обязательном порядке задают вопросы. При этом действуют следующие правила:

Качество и количество задаваемых вопросов (при минимальном качестве) оцениваются преподавателем дополнительно. Учет вопросов производится пофамильно и учитывается в дальнейшем при выставлении итоговой оценки

Количество вопросов не ограничено; вопросы должны задаваться в корректной форме и в рамках прослушанного доклада и иллюстрирующего его материала.

.Каждый студент и преподаватель получают оценочный лист . Оценка работы производится по критериям:

постановка задачи;

качество презентации (доклада, выступления);

ответы на вопросы.

По окончании выступления (после ответов на все интересующие вопросы) всем остальным участникам дается время (2-3 минуты) на выставление оценок в оценочный лист. Оценки выставляются по 10-балльной шкале. Они должны выставляться максимально объективно. Преподаватель лично, либо поручив это созданной из числа студентов счетной комиссии, подводит итог.

Методические рекомендации по выполнению тестов

В тест могут быть включены задания различных типов:

с выбором одного или нескольких верных ответов

с вводом ответа с клавиатуры

на установление соответствия

на упорядочение

на классификацию

В тесте могут сочетаться задания разных типов в любых комбинациях.

Методические рекомендации по выполнению ситуационного задания.

Работа с ситуационными заданиями позволяет рассмотреть варианты решения проблемной практико-ориентированной ситуации с учетом сформированных теоретических знаний и навыков.

Традиционно ситуационное задание содержит схематическое словесное описание ситуации, статистические данные. Задание дает возможность приблизиться к практике, встать на позицию человека, реально принимающего решения, наглядно демонстрируют, как применить теоретические знания к решению практических задач. С помощью этого метода студенты имеют возможность проявить и совершенствовать аналитические и оценочные навыки, находить наиболее рациональное решение поставленной проблемы.

Решение ситуационного задания представляет собой продукт индивидуальной работы студентов. Работа с ситуационным заданием осуществляется поэтапно:

Первый этап – знакомство с текстом ситуационного задания, изложенной в нем ситуацией, его особенностями.

Второй этап – выявление фактов, указывающих на проблему(ы), выделение основной проблемы (основных проблем), выделение факторов и персоналий, которые могут реально воздействовать.

Третий этап – выстраивание иерархии проблем (выделение главной и второстепенных), выбор проблемы, которую необходимо будет решить.

Четвертый этап – генерация вариантов решения проблемы. Возможно проведение «мозгового штурма».

Пятый этап – оценка каждого альтернативного решения и анализ последствий принятия того или иного решения.

Шестой этап – принятие окончательного решения по ситуационному заданию, например, перечня действий или последовательности действий.

Седьмой этап – презентация решения и общее обсуждение.

Восьмой этап - подведение итогов в учебной группе под руководством преподавателя.

Максимальная польза из работы над ситуационным заданием будет извлечена в том случае, если студенты при предварительном знакомстве с ними будут придерживаться систематического подхода к их

анализу, основные шаги которого представлены ниже.

1. Выпишите из соответствующих разделов учебной дисциплины ключевые идеи, для того, чтобы освежить в памяти теоретические концепции и подходы, которые Вам предстоит использовать при анализе кейса.

2. Бегло прочтите текст задания, чтобы составить о нем общее представление.

3. Внимательно прочтите вопросы к заданию и убедитесь в том, что Вы хорошо поняли, что Вас просят сделать.

4. Вновь прочтите текст задания, внимательно фиксируя все факторы или проблемы, имеющие отношение к поставленным вопросам.

5. Продумайте, какие идеи и концепции соотносятся с проблемами, которые Вам предлагается рассмотреть при работе над ситуационным заданием.

Для успешного решения ситуационного задания немаловажным фактором является генерация идей.

Презентация, или представление результатов анализа ситуационного задания, выступает очень важным элементом метода. При этом возможна два вида презентаций: устная (публичная) и письменный отчет-презентация.

Публичная (устная) презентация предполагает представление решения ситуационного задания группе.

Устная презентация требует навыков публичного выступления, умения кратко, но четко и полно изложить информацию, убедительно обосновать предлагаемое решение, корректно отвечать на критику и возражения. Одним из преимуществ публичной (устной) презентации является ее гибкость. Выступающий может откликаться на изменения окружающей обстановки, адаптировать свой стиль и материал, чувствуя настроение аудитории.

Письменный отчет-презентация выполняется с использованием средств LibreOffice и требует проявления таких качеств, как умение подготовить текст, точно и аккуратно составить отчет, не допустить ошибки в расчетах и т.д. Подготовка письменного анализа ситуационного задания аналогична подготовке устного, с той разницей, что письменные отчеты-презентации обычно более структурированы и детализированы. Основное правило письменного анализа ситуационного задания заключается в том, чтобы избегать простого повторения информации из текста, информация должна быть представлена в переработанном виде. Самым важным при этом является собственный анализ представленного материала, его соответствующая интерпретация и сделанные предложения.

При оценке выполнения ситуационного задания преподаватель оценивает:

1. Научно-теоретический уровень выполнения ситуационного задания и выступления.

2. Полнота решения ситуационного задания.

3. Степень творчества и самостоятельности в подходе к анализу ситуационного задания и его решению. Доказательность и убедительность.

4. Форма изложения материала (свободная; своими словами; грамотность устной или письменной речи) и качество презентации.

5. Культура речи, жестов, мимики при устной презентации.

6. Полнота и всесторонность выводов.

7. Наличие собственных взглядов на проблему.