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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Информационная безопасность в системах электронной коммерции

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	8			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Серпенинов О.В.

Зав. кафедрой: к.э.к., доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	сформировать профессиональные компетенции в области обеспечения безопасного функционирования процессов систем электронной коммерции различных классов, в т.ч. согласно требованиям и рекомендациям контролирующих государственных органов

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-2: способен администрировать подсистемы информационной безопасности объекта защиты

В результате освоения дисциплины обучающийся должен:

Знать:

принципы построения систем защиты информации;
критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем;
основные угрозы безопасности информации и модели нарушителя (соотнесено с индикатором ПК-2.1)

Уметь:

анализировать угрозы безопасности информации;
оценивать информационные риски;
применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации;
анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей (соотнесено с индикатором ПК-2.2)

Владеть:

навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах;
навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации (соотнесено с индикатором ПК-2.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы безопасности электронной коммерции

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1.1. «Общие вопросы обеспечения информационной безопасности систем электронной коммерции» :основные понятия;цели и задачи; преимущества и недостатки по сравнению с традиционной коммерцией; модели B2B, B2C, C2C / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Тема 1.1. «Общие вопросы обеспечения информационной безопасности систем электронной коммерции»: лабораторная работа по теме лекции с использованием LibreOffice / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Тема 1.1. «Общие вопросы обеспечения информационной безопасности систем электронной коммерции»: самостоятельная работа по теме лекции / Ср /	8	8	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Тема 1.2. «Правовые основы обеспечения информационной безопасности электронной коммерции»:состав и структура органов власти, осуществляющих контроль и надзор; федеральные законы, постановления Правительства, указы Президента РФ, ведомственные акты, государственные стандарты, международное законодательство. / Лек /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Тема 1.2. «Правовые основы обеспечения информационной безопасности электронной коммерции»:лабораторная работа по теме лекции с использованием LibreOffice / Лаб /	8	4	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.6	Тема 1.2. «Правовые основы обеспечения информационной безопасности электронной коммерции»: самостоятельная работа по теме лекции / Ср /	8	4	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.7	Тема 1.3. «Угрозы безопасности систем электронной коммерции»: методы социальной инженерии; удаленные сетевые атаки / Лек /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.8	Тема 1.3. «Угрозы безопасности систем электронной коммерции»:лабораторная работа по теме лекции / Лаб /	8	4	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.9	Тема 1.3. «Угрозы безопасности систем электронной коммерции»: самостоятельная работа по теме лекции / Ср /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4

Раздел 2. Инфраструктура безопасности электронной коммерции

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 2.1. «Аудит безопасности систем электронной коммерции»:понятие, цели, задачи и этапы проведения / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.2	Тема 2.1. «Аудит безопасности систем электронной коммерции»:лабораторная работа по теме лекции / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Тема 2.1. «Аудит безопасности систем электронной коммерции»:: самостоятельная работа по теме лекции / Ср /	8	8	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Тема 2.2. «Требования стандарта Безопасности PCI DSS»:построение и сопровождение защищённой сети; защита данных держателей карт;поддержка программы управления уязвимостями;реализация мер по строгому контролю доступа;регулярный мониторинг и тестирование сети;поддержка политики информационной безопасности / Лек /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Тема 2.2. «Требования стандарта Безопасности PCI DSS»:лабораторная работа по теме лекции / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Тема 2.2. «Требования стандарта Безопасности PCI DSS»: самостоятельная работа по теме лекции / Ср /	8	8	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.7	Тема 2.3. «Методы и средства аудита безопасности систем электронной коммерции»:анализ рисков; анализ соответствия требованиям стандартов; комплексных подход; тестирование на проникновение. / Лек /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.8	Тема 2.3. «Методы и средства аудита безопасности систем электронной коммерции»: лабораторная работа по теме лекции / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.9	Тема 2.3. «Методы и средства аудита безопасности систем электронной коммерции»:самостоятельная работа по теме лекции / Ср /	8	10	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.10	/ Зачёт /	8	0	ПК-2	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Аверченков В. И.	Аудит информационной безопасности: учебное пособие	Москва: ФЛИНТА, 2021	https://biblioclub.ru/index.php?page=book&id=93245 неограниченный доступ для зарегистрированных пользователей
Л1.2	Кобелев О. А., Пирогов С. В.	Электронная коммерция: учебное пособие	Москва: Дашков и К°, 2020	https://biblioclub.ru/index.php?page=book&id=621649 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=238445 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.2	Пакин, А. И.	Информационная безопасность информационных систем управления предприятием: учебное пособие по части курса	Москва: Московская государственная академия водного транспорта, 2009	https://www.iprbookshop.ru/46462.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Бердюгин А. А., Дудка А. Б., Конявская С. В., Конявский В. А., Назаров И. Г., Ревенков П. В.	Кибербезопасность в условиях электронного банкинга: практическое пособие	Москва: Прометей, 2020	https://biblioclub.ru/index.php?page=book&id=610688 неограниченный доступ для зарегистрированных пользователей
Л2.4	Козьминых С. И.	Обеспечение комплексной защиты объектов информатизации: учебное пособие	Москва: Юнити-Дана, 2020	https://biblioclub.ru/index.php?page=book&id=615695 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

"Консультант+" https://www.cosultant.ru/
Бесплатная база данных ГОСТ https://docplan.ru/
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов 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.

Лабораторные работы проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

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-2: способен администрировать подсистемы информационной безопасности объекта защиты			
З: принципы построения систем защиты информации; Критерии оценивания эффективности и надежности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов для подготовке к зачету, опросу	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры на зачете	З (1-40) О (1-40)
У: анализировать угрозы безопасности информации; оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей	использует современные программные средства при выполнении лабораторных и практико-ориентированных заданий	корректный выбор программного средства для выполнения лабораторных и практико-ориентированных заданий	ЛЗ (1-7) ПОЗЗ (1-5)
В: навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации	проводит оценку защищенности и обеспечения информационной безопасности в системах электронной коммерции на высоком уровне при выполнении лабораторных и практико-ориентированных заданий	правильность выполнения лабораторных и практико-ориентированных заданий	ЛЗ (1-7) ПОЗЗ (1-5)

О – опрос, З – вопросы для зачета, ПОЗЗ – практико-ориентированные задания для зачета, ЛЗ – лабораторные задания

1.2 Шкалы оценивания:

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

- 50-100 баллов («зачет»)
- 0-49 баллов («незачет).

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. Актуальность вопросов информационной безопасности в системах электронной коммерции
2. Модели электронной коммерции
3. Риски в системах электронной коммерции
4. Управление безопасностью в системах электронной коммерции
5. Международная практика правового обеспечения систем электронной коммерции
6. Особенности правового регулирования деятельности в области электронной коммерции в РФ
7. Государственные стандарты РФ в области безопасности систем электронной коммерции

8. Международные стандарты безопасности систем электронной коммерции
9. Отраслевые стандарты безопасности систем электронной коммерции
10. Классификация атак на системы электронной коммерции
11. Источники угроз в системах электронной коммерции
12. Модуль угроз в системах электронной коммерции
13. Модель нарушителя в системах электронной коммерции
14. Типовые уязвимости наиболее распространённых CMS в области электронной коммерции
15. Этапы проведения типовой атаки
16. Методы социальной инженерии при осуществлении атак на системы электронной коммерции
17. Атаки DDoS
18. SQL-инъекции
19. Обеспечение безопасности транзакций в системах электронной коммерции
20. Цифровые сертификаты
21. Архитектура системы центров сертификации
22. Атаки, направленные на протокол SSL
23. Требования стандарта PCI DSS
24. Уровни сертификации торгово-сервисных предприятий
25. Уровни сертификации поставщиков услуг
26. Особенности протокола 3D Secure
27. Особенности протокола Mir Accept
28. Способы оценки защищенности системы электронной коммерции
29. Оценка защищенности систем электронной коммерции в соответствии с зарубежными стандартами
30. Оценка защищенности систем электронной коммерции в соответствии с российскими стандартами
31. Виды аудита безопасности систем электронной коммерции
32. Цели и задачи аудита безопасности систем электронной коммерции
33. Особенности организационного аудита систем электронной коммерции
34. Особенности инструментального аудита систем электронной коммерции
35. Ключевые этапы аудита безопасности систем электронной коммерции
36. Инструментарий для сбора исходных данных
37. Подходы к анализу данных, собранных в процессе аудита
38. Подходы к разработке рекомендаций по итогам аудита безопасности
39. Отчет по результатам аудита
40. Разработка комплекса мероприятий по повышению уровня защищенности

Типовые практико-ориентированные задания к зачету

1. «Правовые основы обеспечения информационной безопасности электронной коммерции»
2. «Угрозы безопасности систем электронной коммерции»
3. «Аудит безопасности систем электронной коммерции»
4. «Требования стандарта Безопасности PCI DSS»
5. «Методы и средства аудита безопасности систем электронной коммерции»

Критерии оценивания:
- 50-100 баллов (оценка «зачтено») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированных заданий, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 0-49 баллов (оценка «незачтено») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированных заданий, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Лабораторные задания

Лабораторное задание 1. «Общие вопросы обеспечения информационной безопасности систем электронной коммерции».
Лабораторное задание 2. «Правовые основы обеспечения информационной безопасности электронной коммерции».
Лабораторное задание 3. «Угрозы безопасности систем электронной коммерции».
Лабораторное задание 4. «Аудит безопасности систем электронной коммерции».
Лабораторное задание 5. «Требования стандарта Безопасности PCI DSS».
Лабораторное задание 6. «Методы и средства аудита безопасности систем электронной коммерции»
Лабораторное задание 7. Формирование модели нарушителя компьютерных сетей

Критерии оценивания:
(для каждого лабораторного задания)
9-10 б. – задание выполнено верно;
6-8 б. – при выполнении задания были допущены неточности, не влияющие на результат;
3-5 б. – при выполнении задания были допущены ошибки;
1-2 б. – при выполнении задания были допущены существенные ошибки.
0 б. – задание не выполнено.

Максимальное количество баллов за семестр 70.

Опрос

1. Актуальность вопросов информационной безопасности в системах электронной коммерции
2. Модели электронной коммерции
3. Риски в системах электронной коммерции
4. Управление безопасностью в системах электронной коммерции
5. Международная практика правового обеспечения систем электронной коммерции
6. Особенности правового регулирования деятельности в области электронной коммерции в РФ
7. Государственные стандарты РФ в области безопасности систем электронной коммерции
8. Международные стандарты безопасности систем электронной коммерции
9. Отраслевые стандарты безопасности систем электронной коммерции
10. Классификация атак на системы электронной коммерции
11. Источники угроз в системах электронной коммерции
12. Модуль угроз в системах электронной коммерции
13. Модель нарушителя в системах электронной коммерции
14. Типовые уязвимости наиболее распространённых CMS в области электронной коммерции
15. Этапы проведения типовой атаки
16. Методы социальной инженерии при осуществлении атак на системы электронной коммерции
17. Атаки DDoS
18. SQL-инъекции
19. Обеспечение безопасности транзакций в системах электронной коммерции
20. Цифровые сертификаты
21. Архитектура системы центров сертификации
22. Атаки, направленные на протокол SSL
23. Требования стандарта PCI DSS
24. Уровни сертификации торгово-сервисных предприятий
25. Уровни сертификации поставщиков услуг
26. Особенности протокола 3D Secure
27. Особенности протокола Mir Accept
28. Способы оценки защищенности системы электронной коммерции
29. Оценка защищенности систем электронной коммерции в соответствии с зарубежными стандартами

30. Оценка защищенности систем электронной коммерции в соответствии с российскими стандартами
31. Виды аудита безопасности систем электронной коммерции
32. Цели и задачи аудита безопасности систем электронной коммерции
33. Особенности организационного аудита систем электронной коммерции
34. Особенности инструментального аудита систем электронной коммерции
35. Ключевые этапы аудита безопасности систем электронной коммерции
36. Инструментарий для сбора исходных данных
37. Подходы к анализу данных, собранных в процессе аудита
38. Подходы к разработке рекомендаций по итогам аудита безопасности
39. Отчет по результатам аудита
40. Разработка комплекса мероприятий по повышению уровня защищенности

Критерии оценивания:

• 1 балл выставляется обучающемуся за один вопрос, если изложенный материал фактически верен и логически обоснован.
• 0 баллов, если ответ неверный.
Максимальное количество баллов за семестр: 30 баллов

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 виде опросов. Количество вопросов – 3. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются теоретические вопросы с учетом практико-ориентированности изучаемой дисциплины, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки работы с компьютером, применения методов и технологий защиты информации.

При подготовке к лабораторным занятиям каждый обучающийся должен:

– изучить рекомендованную учебную литературу;

– изучить практические примеры, рассмотренные на лекциях;

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

Вопросы, не рассмотренные на лекциях, лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом опроса или при выполнении лабораторных заданий. 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. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному 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.