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

УТВЕРЖДАЮ
Начальник отдела лицензирования и аккредитации
_____Чаленко К.Н.
«____» _____ 20___г.

Рабочая программа дисциплины
Основы информационной безопасности

38.05.01 Экономическая безопасность
38.05.01.01 "Экономико-правовое обеспечение экономической безопасности"

Для набора 2021, 2022 гг.

Квалификация
Экономист

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	76	76	76	76
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 26.04.2022 протокол № 9/1.

Программу составил(и): к.э.н., доцент, Шарыпова Т.Н. _____

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____

Методическим советом направления: дэн, профессор, Суржиков М.А. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений; расширение кругозора.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-6:Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

В результате освоения дисциплины обучающийся должен:

Знать:

методы и средства для сбора, анализа, систематизации и оценки данных, необходимых для решения профессиональных задач.

Уметь:

осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных для решения профессиональных задач.

Владеть:

применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Общие вопросы информационной безопасности				
1.1	Тема 1 «Введение в информационную безопасность". Понятие информации, защиты информации, информационной системы, информационной безопасности. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Тема 1 «Введение в информационную безопасность". Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора LibreOffice. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Тема 1 "Введение в информационную безопасность". Правовая защита информации. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Тема 2 «Санкционированный и несанкционированный доступ». Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Неформальная модель нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Тема 2 «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации (НСД). Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора LibreOffice. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Тема 2 «Санкционированный и несанкционированный доступ». Административная защита информации. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

1.7	Тема 3 «Понятие угрозы, уязвимости, риска». Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации в юриспруденции. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.8	Тема 3 «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией в LibreOffice. Поиск, сохранение информации, проверка на вирусы. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.9	Тема 3. «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.10	Тема 4 «Ценность информации». Понятие ценности информации. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.11	Тема 4 «Ценность информации». Способы защиты информации на ПК. Вирусы, антивирусные программы с использованием текстового редактора LibreOffice. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.12	Тема 4 «Ценность информации». Административная защита информации. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Методы и средства криптографической защиты				
2.1	Тема 1 «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Тема 1 «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Тема 1 «Принципы криптографической защиты информации». Таблица Вижинера. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.4	Тема 2 «Элементы криптоанализа». Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.5	Тема 2 «Элементы криптоанализа». Метод встречи в середине атаки. Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.6	Тема 2 «Элементы криптоанализа». Особенности использования вычислительной техники в криптографии. /Ср/	6	10	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.7	Тема 3 «Симметричные криптосистемы». Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Недостатки симметричных криптосистем. Основные виды симметричных шифров. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.8	Тема 3 «Симметричные криптосистемы». Система шифрования Цезаря. Шифры перестановки. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.9	Тема 3 «Симметричные криптосистемы». Шифр Гронсфельда. Шифры многоалфавитной замены. /Ср/	6	8	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

2.10	Тема 4 «Асимметричные криптосистемы». Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена. Достоинства и недостатки асимметричных криптосистем. Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA. /Лек/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.11	Тема 4 «Асимметричные криптосистемы». Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений с использованием текстового редактора LibreOffice. /Лаб/	6	2	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.12	Тема 4 «Асимметричные криптосистемы». Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. /Ср/	6	8	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.13	/Зачёт/	6	0	ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

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, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	https://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=230502 неограниченный доступ для зарегистрированных пользователей
Л2.2	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	http://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Консультант Плюс"

Информационная система "Единое окно доступа к образовательным ресурсам". http://window.edu.ru/

Бесплатная база данных ГОСТ. https://docplan.ru/

5.4. Перечень программного обеспечения

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 (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия 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 (МОДУЛЯ)

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
ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач			
З: методы и средства для сбора, анализа, систематизации и оценки данных, необходимых для решения профессиональных задач	изучает основную и дополнительную литературу, лекционный материал; знает основные источники и правила доступа, а также использования информации, в том числе в профессиональных целях; знает основные методы хранения и обработки информации, а также ее трансляции при подготовке к тестированию, зачету	соответствие ответов материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет; сформировавшееся систематическое знание основных источников и правил доступа, а также использования информации, в том числе в профессиональных целях; основных методов хранения и обработки информации, а также ее трансляции при ответе на вопросы тестирования, зачета	Т (Раздел 1; Раздел 2), З (вопросы 1-67)
У: осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных для решения профессиональных задач	умеет находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку для решения лабораторных и практико-ориентированных заданий	сформировавшееся систематическое умение находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (Раздел 1); ПОЗЗ (раздел 1)
В: применять основные методы, способы и средства получения, хранения, поиска, систематизации,	обладает навыками использования современных информационно-коммуникационных технологий и различных информационных ресурсов	сформировавшееся систематическое владение навыками использования современных информационно-коммуникационных технологий и различных	ЛЗ (Раздел 2); ПОЗЗ (раздел 2)

обработки и передачи информации	для решения лабораторных и практико-ориентированных заданий	информационных ресурсов при выполнении лабораторных и практико-ориентированных заданий	

Т – тест, ЛЗ – лабораторные задания, ПОЗЗ - практико-ориентированные задания к зачету, *З-вопросы к зачету.*

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. Понятие информации, защиты информации, информационной системы, информационной безопасности.
2. Цель защиты информации.
3. Базовые свойства информации: конфиденциальность, целостность, доступность.
4. Нормативно-правовая база функционирования систем защиты информации.
5. Российское законодательство по защите информационных технологий.
6. Правовая защита программного обеспечения авторским правом.
7. Компьютерные преступления и особенности их расследования.
8. Правовая защита информации.
9. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
10. Неформальная модель нарушителя.
11. Причины несанкционированного доступа к информации.
12. Последствия несанкционированного доступа к информации.
13. Несанкционированный доступ к информации (НСД).
14. Идентификация. Аутентификация. Выбор паролей.
15. Административная защита информации.
16. Понятие угрозы, классификация угроз.
17. Понятие уязвимости, атаки на компьютерную систему.
18. Понятие риска.
19. Виды утечки информации в юриспруденции.
20. Понятие канала утечки информации, основные каналы утечки информации.
21. Классификация злоумышленников.
22. Уязвимость компьютерных систем.
23. Технологии организации работы с информацией в среде LibreOffice.

24. Поиск, сохранение информации, проверка на вирусы.
25. Понятие ценности информации.
26. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
27. Способы защиты информации на ПК.
28. Вирусы, антивирусные программы.
29. Административная защита информации.
30. Особенности парольных систем, основные типы угроз безопасности парольных систем.
31. Требования к выбору и использованию паролей.
32. Архиваторы. Архивы. Методы сжатия архиваторов.
33. Сегментирование.
34. Возможности ОС по созданию учетной записи пользователя с ограниченными правами.
35. Порядок удаления ограниченной учетной записи.
36. Защита электронной почты.
37. Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма.
38. Принципы функционирования криптографической системы.
39. Классификация криптосистем.
40. Процесс шифрования текста с помощью таблицы Вижинера.
41. Расшифровка текста с помощью таблицы Вижинера.
42. Понятие криптоанализа, криптоаналитической атаки.
43. Основные типы криптоаналитических атак, криптостойкость шифра.
44. Требования к шифрам, используемым для криптографической защиты информации.
45. Метод встречи в середине атаки.
46. Вероятностный метод криптоанализа.
47. Анализ возможности возникновения коллизии.
48. Особенности использования вычислительной техники в криптографии.
49. Принцип функционирования симметричных криптосистем.
50. Функциональная схема взаимодействия участников симметричного криптографического обмена.
51. Недостатки симметричных криптосистем.
52. Основные виды симметричных шифров.
53. Система шифрования Цезаря.
54. Шифры перестановки.
55. Шифр Гронсфельда.
56. Шифры многоалфавитной замены.
57. Принцип функционирования асимметричных криптосистем. Функциональная схема взаимодействия участников асимметричного криптографического обмена.
58. Достоинства и недостатки асимметричных криптосистем.
59. Реализация двустороннего обмена ключевой информацией.
60. Понятие и назначение центра распределения ключей.
61. Требования Диффи и Хеллмана.
62. Алгоритм шифрования RSA.
63. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

64. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).

65. Целостность передаваемых данных.

66. Авторство сообщений. Основные математические соотношения, используемые в алгоритме RSA.

67. Технология взлома шифра методом полного перебора.

Практико-ориентированные задания к зачету

Раздел 1 «Общие вопросы информационной безопасности».

1. Выполнить установку антивирусной программы.
2. Создать учетную запись пользователя с ограниченными правами.
3. Выполнить защиту электронной почты.
4. Выполнить сегментирование.
5. Выполнить установку паролей.
6. Выполнить удаление ограниченной учетной записи.

Раздел 2. «Методы и средства криптографической защиты».

1.С помощью алгоритма RSA зашифровать слово ДЕРЕВО (4.9.5). Для реализации алгоритма использовать числа p=19, q=29.

2.С помощью алгоритма RSA зашифровать слово ОСЕНЬ (2. 6.4). Для реализации алгоритма использовать числа p=17, q=29.

3.С помощью алгоритма RSA зашифровать слово СОЛНЦЕ (5. 6. 3. 1). Для реализации алгоритма использовать числа p=13, q=31.

4.С помощью алгоритма RSA зашифровать слово УТРО (1.9.2.4). Для реализации алгоритма использовать числа p=11, q=19.

5.С помощью алгоритма RSA зашифровать слово КОШКА (6. 5. 1). Для реализации алгоритма использовать числа p=11, q=13.

6. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ГРУША – ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Критерии оценивания:

- 50-100 баллов («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 («не зачтено») – 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

1.Тематика лабораторных заданий по разделам и темам

Раздел 1 «Общие вопросы информационной безопасности».

Тема 1 «Введение в информационную безопасность».

Лабораторное задание 1 «Нормативно-правовая база функционирования систем защиты информации». Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора LibreOffice.

Тема 2 «Санкционированный и несанкционированный доступ».

Лабораторное задание 2 «Несанкционированный доступ к информации (НСД)». Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора LibreOffice.

Тема 3 «Понятие угрозы, уязвимости, риска».

Лабораторное задание 3 «Технологии организации работы с информацией в LibreOffice». Поиск, сохранение информации, проверка на вирусы.

Тема 4 «Ценность информации».

Лабораторное задание 4 «Способы защиты информации на ПК». Вирусы, антивирусные программы с использованием текстового редактора LibreOffice.

Раздел 2 «Методы и средства криптографической защиты»

Тема 1. «Принципы криптографической защиты информации».

Лабораторное задание 1 «Процесс шифрования текста с помощью таблицы Вижинера». Расшифровка текста с помощью таблицы Вижинера.

Тема 2 «Элементы криптоанализа».

Лабораторное задание 2 «Метод встречи в середине атаки». Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии.

Тема 3 «Симметричные криптосистемы».

Лабораторное задание 3 «Система шифрования Цезаря». Шифры перестановки.

Тема 4 «Асимметричные криптосистемы».

Лабораторное задание 4 «Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП)». Целостность передаваемых данных. Авторство сообщений с использованием текстового редактора LibreOffice.

2. Критерии оценивания:

Максимальное количество баллов: 72 балла.

Каждое задание оценивается максимум в 9 баллов.

9 б. – задание выполнено верно;

8-6 б. – при выполнении задания были допущены неточности, не влияющие на результат;

5-3 б. – при выполнении задания были допущены ошибки;

2-1 б. – при выполнении задания были допущены существенные ошибки.

0 б. – задание не выполнено.

Тесты

1. Банк тестов по разделам и (или) темам

Раздел 1 «Общие вопросы информационной безопасности».

Тема 1 «Введение в информационную безопасность».

1.К правовым методам, обеспечивающим информационную безопасность, относятся:

a) разработка аппаратных средств обеспечения правовых данных

b) разработка и установка во всех компьютерных правовых сетях журналов учета действий

c) разработка и конкретизация правовых нормативных актов обеспечения безопасности

2.**Виды информационной безопасности:**

a) персональная, корпоративная, государственная
b) клиентская, серверная, сетевая
c) локальная, глобальная, смешанная

3. **Основные объекты информационной безопасности:**

a) компьютерные сети, базы данных
b) информационные системы, психологическое состояние пользователей
c) бизнес-ориентированные, коммерческие системы

Тема 2 «Санкционированный и несанкционированный доступ».

1.Угроза информационной системе (компьютерной сети) – это:

a) вероятное событие
b) детерминированное (всегда определенное) событие
c) событие, происходящее периодически

2. **Наиболее распространены средства воздействия на сеть офиса:**

a) слабый трафик, информационный обман, вирусы в интернет
b) вирусы в сети, логические мины (закладки), информационный перехват
c) компьютерные сбои, изменение администрирования, топологии.

Тема 3 «Понятие угрозы, уязвимости, риска».

1. **Основными источниками угроз информационной безопасности являются все указанное в списке:**

a) хищение жестких дисков, подключение к сети, инсайдерство
b) перехват данных, хищение данных, изменение архитектуры системы
c) хищение данных, подкуп системных администраторов, нарушение регламента работы

2. **Угроза информационной системе (компьютерной сети) – это:**

a) вероятное событие
b) детерминированное (всегда определенное) событие
c) событие, происходящее периодически

Тема 4 «Ценность информации».

1.Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

a) программные, технические, организационные, технологические
b) серверные, клиентские, спутниковые, наземные
c) личные, корпоративные, социальные, национальные

2. К основным принципам обеспечения информационной безопасности относится:

a) экономической эффективности системы безопасности
b) многоплатформенной реализации системы
c) усиления защищенности всех звеньев системы

Раздел 2 «Методы и средства криптографической защиты»

Тема 1. «Принципы криптографической защиты информации».

1.Что представляет собой криптографическая система?

a) семейство T преобразований открытого текста, члены его семейства индексируются символом k
b) программу
c) систему

2.Требования, предъявляемые к современным криптографическим системам защиты информации:
a) знание алгоритма шифрования не должно влиять на надежность защиты
b) структурные элементы алгоритма шифрования должны быть неизменными
c) не должно быть простых и легко устанавливаемых зависимостью между ключами
d) последовательно используемыми в процессе шифрования

Тема 2 «Элементы криптоанализа».

1. Цель криптоанализа:
a) определение стойкости алгоритма
b) увеличение количества функций замещения в криптографическом алгоритме
c) уменьшение количества функций подстановок в криптографическом алгоритме
d) определение использованных перестановок

2. Выберите правильное определение термина «криптоанализ»
a) криптоанализ – это наука о преодолении криптографической защиты информации
b) криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи
c) криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
d) криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации

Тема 3 «Симметричные криптосистемы».

1. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
a) 1
b) 2
c) 3

2. Какой алгоритм не используется при симметричном шифровании:
a) поточное шифрование
b) побитовое шифрование
c) блочное шифрование
d) алгоритм Эль-Гамаля

3. Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:
a) режим гаммировани
b) режим простой замены
c) режим обратной связи по шифротексту
d) режим гаммирования с обратной связью

Тема 4 «Асимметричные криптосистемы».

1. Асимметричные алгоритмы шифрования по-другому называются
   a) алгоритмами шифрования с открытым ключом
   b) симметричными алгоритмами шифрования
   c) односторонними алгоритмами шифрования
   d) помехоустойчивыми алгоритмами шифрования

2.Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для формирования электронной цифровой подписи?

a) отправитель использует для шифрования открытый ключ получателя, а получатель использует для расшифрования свой закрытый ключ

b) отправитель использует для шифрования закрытый ключ получателя, а получатель использует для расшифрования свой открытый ключ

c) отправитель использует для шифрования свой открытый ключ, а получатель использует для расшифрования закрытый ключ отправителя

d) отправитель использует для шифрования свой закрытый ключ, а получатель использует для расшифрования открытый ключ отправителя

2.Инструкция по выполнению

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 14 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 40 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

3. Критерии оценивания:

Максимальное количество баллов: 28 баллов.

23-28 баллов - выставляется студенту, если он правильно ответил не менее, чем на 85% вопросов теста;

18-22 баллов - выставляется студенту, если он правильно ответил не менее, чем на 67% вопросов теста;

14-17 баллов - выставляется студенту, если он правильно ответил не менее, чем на 50% вопросов теста;

0-13 баллов - выставляется студенту, если он правильно ответил менее, чем на 50% вопросов теста.

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 окончанию теоретического обучения до начала экзаменационной сессии в соответствии с расписанием. Количество вопросов в задании – 3: два теоретических вопроса и одно практико-ориентированное задание. 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

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются вопросы информационной безопасности, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки получения, хранения, переработки информации и работы с компьютером как со средством управления информацией.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на лабораторных 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 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.