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
Защита информационных процессов и систем

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 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	48	48	48	48
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

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

Программу составил(и): доцент, Прохоров А.И.

Зав. кафедрой: к.э.н.,доцент Радченко Ю.В.

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации

В результате освоения дисциплины обучающийся должен:

Знать:

Основы криптографии, особенности различных операционных систем (соотнесено с индикатором ПК-1.1)

Уметь:

устанавливать системы криптографической защиты информации и операционных систем (соотнесено с индикатором ПК-1.2)

Владеть:

навыками настройки средств криптографической защиты информации в соответствии с требованиями государственных стандартов, обслуживание операционных систем (соотнесено с индикатором ПК-1.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные составляющие и угрозы информационной безопасности (ИБ).

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение: сущность и понятие ИБ; значение ИБ и ее место в системе национальной безопасности / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
1.2	Основные определения: основные составляющие ИБ, основные принципы обеспечения ИБ. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
1.3	Угрозы информационной безопасности: основные определения и классификация угроз, основные угрозы доступности. / Лек /	6	2	ПК-1	Л1.2, Л1.3, Л2.1, Л2.2
1.4	Защита баз данных: создание SQL − сервера с использованием пакета Firebird / Пр /	6	4	ПК-1	Л1.2, Л1.3, Л2.1, Л2.2
1.5	Управление защитой баз данных: управление SQL − сервером с использованием пакета Firebird / Пр /	6	4	ПК-1	Л1.3, Л2.1, Л2.2
1.6	Особенности построений информационной безопасности: анализ угроз основным составляющим ИБ. / Ср /	6	8	ПК-1	Л1.3, Л2.1, Л2.2

Раздел 2. Анализ целей и средств злоумышленников в компьютерных сетях

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Удаленные сетевые атаки: классификация категорий хакеров (злоумышленников) и их целей. Организационно-коммуникативные средства НСД в компьютерную систему. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
2.2	Защита от несанкционированного доступа: средства НСД в компьютерную систему: технические, программные. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
2.3	Защита сетевого взаимодействия: основные сведения об угрозах сетевого взаимодействия; анализ уязвимости информационных систем (ИС). / Лек /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
2.4	Сетевые атаки: классификация сетевых атак и анализ особенностей их организации. / Лек /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
2.5	Системы контроля доступа: управление правами доступа / Пр /	6	4	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
2.6	Системы управления доступом: управление правами доступа в ЛВС / Пр /	6	4	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
2.7	Защита локальной вычислительной сети: неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС, раскрытие и неавторизованная модификация данных и программ. / Ср /	6	4	ПК-1	Л1.2, Л1.3, Л2.1, Л2.2

Раздел 3. Защита операционных систем: специфика безопасности локальных вычислительных сетей (ЛВС) и информационных систем.

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Защита локальной вычислительной сети от модификации: неавторизованный доступ к ЛВС, НСД к ресурсам ЛВС, раскрытие и неавторизованная модификация данных и программ. / Лек /	6	2	ПК-1	Л1.2, Л2.1, Л2.2
3.2	Защита трафика локальной вычислительной сети: раскрытие и подмена трафика ЛВС, разрушение функций ЛВС, ошибки в программном обеспечении, контроль удаленных вычислений. / Лек /	6	2	ПК-1	Л1.3, Л2.1, Л2.2
3.3	Резервное копирование данных: подготовка к резервному копированию базы данных / Пр /	6	4	ПК-1	Л1.3, Л2.1, Л2.2
3.4	Деструктивные воздействия на локальную вычислительную сеть: разрушение функций ЛВС, ошибки в программном обеспечении. Контроль удаленных вычислений. / Ср /	6	4	ПК-1	Л1.2, Л1.3, Л2.1, Л2.2
Раздел 4. Программно-техническая защита: основные программно-технические меры защиты информационных процессов и программного обеспечения (ПО)					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
4.1	Архитектурная безопасность: основные понятия программно-технического уровня ИБ, особенности ИБ современных ИС, архитектурная безопасность. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
4.2	Структурная схема системы ЗИ в типовой ИС: основные функции уровней ЗИ в ИС. / Лек /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
4.3	Средства собственной защиты ПО: средства защиты в составе вычислительной системы, средства защиты с запросом информации. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
4.4	Типы защиты программного обеспечения: средства активной защиты ПО, средства пассивной защиты. / Лек /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
4.5	Защита СУБД: резервное копирование базы данных / Пр /	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
4.6	Защита в *nix-системах: управление Unix − подобной системой. / Пр /	6	4	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
4.7	Собственная защита: средства собственной защиты. / Ср /	6	8	ПК-1	Л1.3, Л2.1, Л2.2
Раздел 5. Структура требований к средствам защиты: основные категории требований к программной и программно-аппаратной реализации средств защиты информации.					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
5.1	Общие требования по обеспечению ИБ: требования к программно-аппаратным средствам, требования к информационным подсистемам (идентификации и аутентификации, управления доступом). / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
5.2	Общие требования к информационным подсистемам (протоколирования, аудита и т.д.), требования к средствам управления ИБ, требования к межсетевому экрану. / Лек /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
5.3	Виртуализация: установка сервера на виртуальную машину. / Пр /	6	4	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
5.4	Встроенные средства защиты: средства защиты в составе вычислительной системы. / Ср /	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
Раздел 6. Требования к защите автоматизированных систем (АС) от НСД.					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
6.1	Основные характеристики технических средств защиты от НСД: основные подсистемы ЗИ от НСД для АС (управления доступом, регистрации и учета, криптографическая, обеспечения целостности) и требования к ним. / Лек /	6	2	ПК-1	Л1.2, Л1.3, Л2.1, Л2.2
6.2	Анализ защищенности: показатели защищенности информации от НСД для компьютерных систем / Пр /	6	2	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
6.3	Межсетевые экраны: показатели защищенности межсетевых экранов. / Пр /	6	2	ПК-1	Л1.1, Л1.3, Л2.1, Л2.2
6.4	Защита от сетевых атак: организация и отражение сетевых атак / Пр /	6	4	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2
6.5	Активная интерфейсная защита: средства защиты с запросом	6	8	ПК-1	Л1.1, Л1.2, Л1.3,

	информации. Средства активной защиты. / Пр /				Л2.1, Л2.2
6.6	/ Экзамен /	6	36	ПК-1	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2

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	Хорев П. Б.	Программно-аппаратная защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информ. безопасность"	М.: ФОРУМ, 2015	25
Л1.2	Завгородний В. И.	Комплексная защита информации в компьютерных системах: Учеб. пособие	М.: Логос, 2001	49
Л1.3	Артемов А. В.	Информационная безопасность: курс лекций: курс лекций	Орел: Межрегиональная академия безопасности и выживания, 2014	https://biblioclub.ru/index.php?page=book&id=428605 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Тищенко Е. Н.	Основы информационной безопасности: учеб.-метод. разраб.	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2012	10
Л2.2	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

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная система "Гарант"
База данных Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Межсетевой экран PFSense
Firebird
Операционная система RedOS
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 занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми

лицензионными и/или свободно распространяемыми 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-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации			
Знать концепцию и принципы построения программного обеспечения, в том числе криптографического.	Описывает способы решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации при ответе на вопросы	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-68) Вопросы к экзамену (вопросы 1-101)
Уметь устанавливать и конфигурировать операционные системы, серверное программное обеспечение и базы данных.	Анализирует состояние системы защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Практико-ориентированные задания (задания 1-35) Практико-ориентированные задания к экзамену (задания 1-8)
Владеть информацией о действующих стандартах и нормативных требований в области информационной	Использует методы и средства защиты информации в соответствии с правовыми	полнота и содержательность ответа умение приводить примеры умение	Практико-ориентированные задания (задания 1-35) Практико-ориентированные

безопасности	нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	самостоятельно находить решение поставленных задач	задания к экзамену (задания 1-8)

1.2 Шкалы оценивания:

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

84-100 баллов (оценка «отлично»)

67-83 баллов (оценка «хорошо»)

50-66 баллов (оценка «удовлетворительно»)

0-49 баллов (оценка «неудовлетворительно»)

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 экзамену

1. Что такое Информационная Безопасность (ИБ), как она относится к Национальной Безопасности?
2. Почему важна ИБ в современном мире?
3. Какие являются основными составными частями ИБ?
4. Можете ли вы перечислить основные принципы обеспечения ИБ?
5. Какова классификация угроз ИБ?
6. Какие являются основными угрозами доступности информации?
7. Как создать SQL-сервер с помощью пакета Firebird?
8. Как управлять SQL-сервером с помощью пакета Firebird?
9. Методы анализа угроз основным компонентам ИБ?
10. Кто такие хакеры (злоумышленники) и что является их целями?
11. Как организованы оргранизационно-коммуникативные средства Национальной Системы Защиты (НСЗ) в компьютерную систему?
12. Какие меры НСД существуют для защиты компьютерных систем?
13. Что нужно знать об угрозах сетевого взаимодействия?
14. Как классифицируются сетевые атаки и как они организуются?
15. Как управлять правами доступа в системе?
16. Как предотвратить неавторизованный доступ к ЛВС?

17. Как защититься от раскрытия и неавторизованной модификации данных и программ в ЛВС?
18. Как готовиться к резервному копированию базы данных?
19. Как бороться с деструктивными воздействиями на ЛВС?
20. Что такое программно-технический уровень ИБ?
21. Какова роль архитектурной безопасности в современных ИС?
22. Как установить сервер на виртуальную машину?
23. Какие требования предъявляются к программно-аппаратным средствам, информационным подсистемам, средствам управления ИБ, межсетевым экранам?
24. Что представляют собой средства собственной защиты?
25. Какие средства защиты включены в состав вычислительных систем?
26. Какие подсистемы защиты существуют для Автоматизированных Систем (АС)?
27. Какие требования предъявляются к этим подсистемам?
28. Как измеряется защищенность информации от НСД для компьютерных систем?
29. Как оценивать защищенность межсетевых экранов?
30. Как организовать и отразить сетевые атаки?
31. Какие средства используются для защиты с запросом информации?
32. Какие средства активной защиты существуют?
33. Различите между активной и пассивной защитой ПО.
34. Как производится резервное копирование базы данных?
35. Как управлять Unix-подобными системами?
36. Какие средства собственной защиты существуют?
37. Какие показатели защищенности имеют межсетевые экраны?
38. Как выполняется планирование мероприятий по противодействию угрозам ИБ?
39. Как происходит мониторинг и анализ угроз ИБ?
40. Какие нормативные правовые акты регламентируют область ИБ в России?
41. Как ведется расследование и сбор улик после нарушения ИБ?
42. Как происходит восстановление работоспособности системы после нарушения ИБ?
43. Как формируется структура отдела ИБ в компании?
44. Какой персонал необходим для работы в отделе ИБ?
45. Классификация угроз ИБ;
46. Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
47. Состав и краткая характеристика основных угроз доступности;
48. Состав и краткая характеристика основных угроз целостности;
49. Состав и краткая характеристика основных угроз конфиденциальности;
50. Классификация категорий хакеров и их целей;
51. Состав и краткая характеристика организационно коммуникативных средств НСД;
52. Состав и краткая характеристика технических средств НСД;
53. Состав и краткая характеристика программных средств НСД;
54. Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
55. Классификация сетевых атак;
56.
57. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
58. Определение IP спуфинга и характеристика основных средств защиты от него;
59. Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
60. Определение парольных атак и характеристика основных средств защиты от них;
61. Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;

62. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
63. Основные методы и условия неавторизованного доступа к ЛВС;
64. Краткая характеристика основных условий НСД к ЛВС;
65. Краткая характеристика основных условий раскрытия данных ЛВС;
66. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
67. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
68. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
69. Основные сервисы безопасности;
70. Основные принципы архитектурной безопасности и их краткая характеристика;
71. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
72. Основные функции централизованного управления рисками и администрирования системы безопасности;
73. Основные функции защиты управления приложениями;
74. Основные функции защиты системы сетей;
75. Основные функции защиты конечных пользователей;
76. Классификация средств защиты программного обеспечения и характеристика их основных категорий;
77. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
78. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
79. Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
80. Классификация средства защиты с запросом информации и характеристика их основных составляющих;
81. Назначение и принцип формирования паролей, шифров, сигнатур;
82. Назначение и основные принципы построения аппаратуры защиты;
83. Классификация средств активной защиты и характеристика их основных составляющих;
84. Определение и характеристика основных внутренних средств активной защиты;
85. Определение и характеристика основных внешних средств активной защиты;
86. Классификация средств пассивной защиты и характеристика их основных составляющих;
87. Назначение и основные принципы организации идентификации программ;
88. Назначение и основные принципы построения устройств контроля;
89. Общий состав требований по обеспечению ИБ;
90. Требования к программно аппаратным средствам;
91. Требования к подсистеме идентификации и аутентификации;
92. Требования к подсистеме управления доступом;
93. Требования к подсистеме протоколирования аудита;
94. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
95. Требования к средствам обеспечения целостности;
96. Требования к средствам управления ИБ;
97. Общий состав требований к межсетевому экрану;
98. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;

99. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
100. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
101. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;

Практико-ориентированные задания к экзамену

1. Создание своей базы данных с помощью пакета Firebird.
2. Управление пользователями и правами доступа в created базе данных с помощью пакета Firebird.
3. Анализ угроз своим IT-инфраструктуре и разработка план действий по борьбе с ними.
4. Изучение различных категорий хакеров и их целей, а также проведение тестовых удаленных сетевых атак на свою систему.
5. Настройка технических и программных средств защиты от несанкционированного доступа к своей компьютерной системе.
6. Изучение уязвимостей своей информационной системы и проведение анализа рисков.
7. Изучение различных типов сетевых атак и разработка плана отражения атак на свою систему.
8. Настройка системы контроля доступа и управления правами доступа в своей локальной вычислительной сети.
9. Настройка мер по защите данных и программ в своей локальной вычислительной сети от несанкционированного доступа и изменения.
10. Настройка мер по защите трафика в своей локальной вычислительной сети.
11. Выполнение резервного копирования своих данных и разработка плана восстановления в случае кражи или уничтожения данных.
12. Изучение архитектуры своей информационной системы и разработка плана по ее защите.
13. Изучение особенностей современных ИС и разработка плана защиты от новых угроз.
14. Разработка политик и процедур по обеспечению информационной безопасности в своей организации.
15. Изучение межсетевых экранов и выбор подходящего решения для своей организации.
16. Изучение встроенных средств защиты в своей вычислительной системе и их настройка.
17. Анализ защищенности своей компьютерной системы и разработка плана по улучшению ее безопасности.

Экзаменационное задание включает 2 теоретических вопроса (раздел «Вопросы к экзамену») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к экзамену»).

Критерии оценивания:

Максимальное количество баллов за экзаменационное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:

- 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;

- 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;

- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;

- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:

- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.

- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.

- 11-24 балла выставляется, если задание решено частично.

- 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:

- 84-100 баллов (оценка «отлично»)
- 67-83 баллов (оценка «хорошо»)
- 50-66 баллов (оценка «удовлетворительно»)
- 0-49 баллов (оценка «неудовлетворительно»)

Опрос

1. Сущность и понятие информационной безопасности (ИБ);
2. Характеристика основных составляющих ИБ;
3. Значение ИБ для субъектов информационных отношений;
4. Место ИБ в системе национальной безопасности;
5. Основные принципы обеспечения ИБ;
6. Классификация угроз ИБ;
7. Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
8. Состав и краткая характеристика основных угроз доступности;
9. Состав и краткая характеристика основных угроз целостности;
10. Состав и краткая характеристика основных угроз конфиденциальности;
11. Классификация категорий хакеров и их целей;
12. Состав и краткая характеристика организационно коммуникативных средств НСД;
13. Состав и краткая характеристика технических средств НСД;
14. Состав и краткая характеристика программных средств НСД;
15. Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
16. Классификация сетевых атак;
17. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
18. Определение IP спуфинга и характеристика основных средств защиты от него;
19. Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;

20. Определение парольных атак и характеристика основных средств защиты от них;
21. Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
22. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
23. Основные методы и условия неавторизованного доступа к ЛВС;
24. Краткая характеристика основных условий НСД к ЛВС;
25. Краткая характеристика основных условий раскрытия данных ЛВС;
26. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
27. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
28. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
29. Основные сервисы безопасности;
30. Основные принципы архитектурной безопасности и их краткая характеристика;
31. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
32. Основные функции централизованного управления рисками и администрирования системы безопасности;
33. Основные функции защиты управления приложениями;
34. Основные функции защиты системы сетей;
35. Основные функции защиты конечных пользователей;
36. Классификация средств защиты программного обеспечения и характеристика их основных категорий;
37. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
38. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
39. Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
40. Классификация средства защиты с запросом информации и характеристика их основных составляющих;
41. Назначение и принцип формирования паролей, шифров, сигнатур;
42. Назначение и основные принципы построения аппаратуры защиты;
43. Классификация средств активной защиты и характеристика их основных составляющих;
44. Определение и характеристика основных внутренних средств активной защиты;
45. Определение и характеристика основных внешних средств активной защиты;
46. Классификация средств пассивной защиты и характеристика их основных составляющих;
47. Назначение и основные принципы организации идентификации программ;
48. Назначение и основные принципы построения устройств контроля;
49. Общий состав требований по обеспечению ИБ;
50. Требования к программно аппаратным средствам;
51. Требования к подсистеме идентификации и аутентификации;
52. Требования к подсистеме управления доступом;
53. Требования к подсистеме протоколирования аудита;
54. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
55. Требования к средствам обеспечения целостности;
56. Требования к средствам управления ИБ;
57. Общий состав требований к межсетевому экрану;

58. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
59. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
60. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
61. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
62. Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.
63. Вопросы для подготовки к экзамену.
64. Сущность и понятие информационной безопасности (ИБ);
65. Характеристика основных составляющих ИБ;
66. Значение ИБ для субъектов информационных отношений;
67. Место ИБ в системе национальной безопасности;
68. Основные принципы обеспечения ИБ;

Критерии оценивания:
Максимальное количество баллов, которое обучающийся может набрать – 40 баллов (за 40 ответов).
Ответ на вопрос оценивается:
- 1 балл – правильный и полный ответ;
- 0 баллов – неправильный ответ или ответ не представлен.

Практикоориентированные задания

1. Написание скриптов на языке SQL для выполнения операций с базой данных, например, создания таблиц, добавления записей, изменения и удаления данных.
2. Настройка системы мониторинга событий в своей ИТ-инфраструктуре и просмотр журналов событий для выявления потенциальных угроз безопасности.
3. Тестирование безопасности web-приложений и API, использующихся в своей организации, с помощью автоматизированных средств, таких как OWASP ZAP или Burp Suite.
4. Разработка политик и процедур по использованию внешних USB-устройств и других съёмных носителей в своей организации.
5. Настройка системы шифрования данных на дисках жесткого drives и в облачных хранилищах.
6. Составление чрезвычайного плана ответа на киберугрозы и проведение учений по его реализации.
7. Изучение и тестирование механизмов двухфакторной аутентификации для доступа к системам и сервисам своей организации.
8. Настройка системы управления учётными записями и паролями для сотрудников своей организации.
9. Изучение и тестирование механизмов печатных маркеров и токенов для аутентификации пользователей в своей организации.
10. Разработка политик и процедур по использованию Wi-Fi сетей в своей организации.
11. Изучение и настройка систем предотвращения вторжений (IDS/IPS) для своей ИТ-инфраструктуры.
12. Тестирование безопасности своих мобильных устройств и разработка политик их использования в своей организации.

13. Изучение и настройка систем обнаружения и коррекции уязвимостей в своей ИТ-инфраструктуре.
14. Разработка политик и процедур по использованию облачных сервисов в своей организации.
15. Настройка системы управления версиями для кода и конфигураций в своей ИТ-инфраструктуре.
16. Тестирование безопасности собственного сайта или веб-приложения путем проведения penetration testing'a или vulnerability scanning'a.
17. Изучение и настройка систем защиты от DDoS-атак для своей ИТ-инфраструктуры.
18. Разработка политик и процедур по безопасному использованию e-mail в своей организации.
19. Изучение и настройка систем логирования и аудита для своей ИТ-инфраструктуры.
20. Разработка политик и процедур по безопасному использованию социальных сетей и мессенджеров в своей организации.
21. Тестирование безопасности удалённого доступа к системам и сервисам своей организации путем проведения remote access testing'a.
22. Изучение и настройка систем автоматизации управления patches и обновлениями для своей ИТ-инфраструктуры.
23. Разработка политик и процедур по использованию VPN в своей организации.
24. Тестирование безопасности стороннего ПО и сервисов, используемых в своей организации, путем проведения code review'a или black box testing'a.
25. Изучение и настройка систем фишинговой защиты и брандмауэров для своей ИТ-инфраструктуры.
26. Разработка политик и процедур по безопасному использованию облачных хранилищ данных в своей организации.
27. Тестирование безопасности баз данных своей организации путем проведения database security testing'a.
28. Изучение и настройка систем безопасности конфигураций для своей ИТ-инфраструктуры.
29. Разработка политик и процедур по использованию IoT-устройств в своей организации.
30. Тестирование безопасности беспроводных сетей своей организации путем проведения wireless network security testing'a.
31. Изучение и настройка систем контроля доступа к файлам и папкам в своей ИТ-инфраструктуре.
32. Разработка политик и процедур по безопасному использованию флеш-накопителей и других съёмных носителей в своей организации.
33. Тестирование безопасности сетевых устройств своей организации путем проведения network device security testing'a.
34. Изучение и настройка систем безопасности облачной инфраструктуры для своей ИТ-инфраструктуры.
35. Разработка политик и процедур по использованию AI и машинного обучения в своей организации.

Критерии оценивания:
Максимальное количество баллов, которое обучающийся может набрать – 60 баллов (за 12 заданий).
Каждое задание оценивается:
- 5 баллов. – задание выполнено верно;
- 4 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 3 баллов. – при выполнении задания были допущены ошибки;
- 2 - 1 баллов. – при выполнении задания были допущены существенные ошибки;

- 0 баллов. – задание не выполнено.

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, экзамена.
Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.
Экзамен проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в экзаменационном задании – 3 (2 теоретических, 1 практико-ориентированное задание). 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;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, 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 решения задач по защите информационных объектов.

При подготовке к практическим занятиям каждый студент должен:
- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием практической работы;
- подготовить ответы на контрольные 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. 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 источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

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.