Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 04.08.2025 22:14:29
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

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
«20» мая 2025 г.

Рабочая программа дисциплины
Методы обеспечения кибербезопасности

Специальность
38.05.01 Экономическая безопасность

Специализация
38.05.01.01 Экономико-правовое обеспечение экономической безопасности

Для набора 2025 года

Квалификация
Экономист

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам / курсам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	40	40	40	40
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.02.2025 г. протокол № 9.

Программу составил(и): доцент, Назарян С.А.

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

Методический совет: д.э.н., доцент М.А. Суржиков

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний в области информационной безопасности и кибербезопасности по организационно-правовой и программно-технической защите коммерческой, служебной, профессиональной тайны, персональных данных; формирование умений и практических навыков по программному и техническому обеспечению личной и корпоративной кибербезопасности при решении задач профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-2. Способен использовать в профессиональной деятельности коммуникационные технологии, государственные и муниципальные информационные системы; осуществлять внутриорганизационные и межведомственные коммуникации необходимые для решения профессиональных задач

В результате освоения дисциплины обучающийся должен:

Знать:

-подходы к самостоятельному поиску информации с использованием различных информационных ресурсов в области обеспечения личной и корпоративной кибербезопасности (соотнесено с индикатором ОПК - 7.1);
-способы решения стандартных задач профессиональной деятельности в области информационной безопасности на основе организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации с применением информационно-коммуникационных технологий (соотнесено с индикатором ПК - 2.1);

Уметь:

-подбирать релевантные технологии обеспечения личной и корпоративной кибербезопасности для решения задач профессиональной деятельности (соотнесено с индикатором ОПК - 7.1);
-использовать современные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе анализа требований нормативно-правовых актов в области обеспечения личной и корпоративной кибербезопасности (соотнесено с индикатором ПК - 2.1);

Владеть:

-применения методик проведения анализа научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности с целью повышения уровня самоорганизации и компетенций в области обеспечения личной и корпоративной кибербезопасности (соотнесено с индикатором ОПК - 7.1);
-навыками организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами контролирующих органов (соотнесено с индикатором ПК - 2.1);

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы информационной безопасности и кибербезопасности

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема "Введение в информационную безопасность и кибербезопасность" Понятийный аппарат в области информационной безопасности и кибербезопасности. Модели информационной безопасности. Целостность, доступность и конфиденциальность. Принципы и направления защиты информации. Правовые основы обеспечения информационной безопасности. Структура и содержание законодательства в области информационной безопасности. Классификация информации по режимам доступа. Информация, доступ к которой не может быть ограничен.Перечень сведений конфиденциального характера. Структура системы организационной защиты информации в РФ. Контролирующие и регулирующие органы.	Лекционные занятия	7	2	ОПК-7 ПК-2
1.2	Тема "Введение в информационную безопасность и кибербезопасность" Пирамида безопасности.Пентагон моделирования угроз. Модель Защиты-Обнаружения-Реагирования. Модель Треугольника угроз.Принцип наименьшей привилегии. Принцип разделения обязанностей. Принцип экономической эффективности. Принцип усиления слабого звена. Принцип эшелонированности обороны. Правовые основы обеспечения информационной безопасности Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их	Самостоятельная работа	7	8	ОПК-7 ПК-2

	расследования. Организация работы со сведениями, отнесенными к государственной тайне. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации."Классификация угроз информационной безопасности" Требования к структуре и содержанию моделей угроз. Нормативные и методические документы ФСТЭК в области моделирования угроз. Технические каналы утечки информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации.				
1.3	Тема "Методы и средства обеспечения информационной безопасности" Правовые методы. Организационные методы. Программно-технические методы. Средства идентификации и аутентификации. Управление доступом. Антивирусное программное обеспечение. Межсетевые экраны. Средства резервирования. Шифрование. Электронная подпись. Кибербезопасность в информационной инфраструктуре организации Нормативные требования и стандарты. Уровни информационной инфраструктуры организации. Особенности реализации угроз на различных уровнях информационной инфраструктуры организации. Последствия реализации угроз. Подбор релевантных мер защиты в соответствии с требованиями регуляторов. Аудит безопасности и тестирование на проникновение. Форензика.	Лекционные занятия	7	2	ОПК-7 ПК-2
1.4	Тема "Методы и средства обеспечения информационной безопасности" Средства централизованного управления и контроля за состоянием информационной безопасности. Средства выявления и предотвращения инсайдерских угроз и рисков утечки информации ограниченного доступа. Искусственный интеллект в задачах обеспечения информационной безопасности. Кибербезопасность в информационной инфраструктуре организации Организация процессов систематического мониторинга состояния кибербезопасности в организации. Подходы к формирования релевантного набора мер защиты.Мероприятия по реализации мер защиты. Методология и способы расследование киберинцидентов.	Самостоятельная работа	7	6	ОПК-7 ПК-2
1.5	Практическое задание 1 Защита информации в пакетах офисных программ LibreOffice. Управление доступом. Защита отдельных объектов содержимого от модификации и удаления. Шифрование. Электронная подпись.	Практические занятия	7	4	ОПК-7 ПК-2
1.6	Практическое задание 3. Инструменты шифрования. Изучение инструментов асимметричного шифрования. Генерация ключевой пары. Шифрование и расшифрование.	Практические занятия	7	4	ОПК-7 ПК-2

Раздел 2. Защита от угроз и конфиденциальность

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	Тема "Методы и средства криптографический защиты информации" Основные понятия и принципы. Классификация. Правовое регулирование. Принципы функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Основные симметричные криптоалгоритмы. Принципы функционирования асимметричных криптосистем. Функциональная схема взаимодействия участников асимметричного криптографического обмена. Основные асимметричные криптоалгоритмы. Достоинства и недостатки симметричных и асимметричных криптосистем. Электронная подпись. Криптостойкость.	Лекционные занятия	7	2	ОПК-7 ПК-2
2.2	Тема "Методы и средства криптографический защиты информации" Классификация атак на криптосистемы. Алгоритмы электронной подписи. Перспективные технологии. Квантовая криптография.	Самостоятельная работа	7	4	ОПК-7 ПК-2
2.3	Тема "Вредоносное программное обеспечение и способы защиты" Компьютерная вирусология. Классификация вредоносного ПО. Последствия вирусных атак. Особенности механизмов воздействия вредоносного ПО. Выявление вредоносного ПО. Антивирусные технологии и их практическое применение.	Лекционные занятия	7	2	ОПК-7 ПК-2
2.4	Тема "Вредоносное программное обеспечение и способы защиты" Развитие и эволюция вредоносного программного обеспечения. Мотивация злоумышленника при использовании вредоносного программного обеспечения. Экономические аспекты и последствия	Самостоятельная работа	7	8	ОПК-7 ПК-2

	атак вредоносного программного обеспечения. Управление уязвимостями и патчинг программного обеспечения.				
2.5	Тема "Защита от удаленных сетевых атак". Функционирование компьютерных сетей. Угрозы и уязвимости. Классификация атак и их характеристика. Последствия атак Способы обнаружения сетевых атак. Способы защиты. Межсетевое экранирование. Технология VPN. Безопасность использования беспроводных сетей.	Лекционные занятия	7	2	ОПК-7 ПК-2
2.6	Тема "Защита от удаленных сетевых атак". Уязвимости веб-приложений: инъекции, кросс-сайтовый скриптинг.Уязвимости операционных систем и сервисов: эксплойты для получения доступа. Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).Использование облачных брандмауэров и антивирусов.Журналирование и мониторинг сетевой активности.Реагирование на инциденты: планы и процедуры.	Самостоятельная работа	7	4	ОПК-7 ПК-2
2.7	Тема "Защита персональных данных в цифровой среде" Источники угроз и каналы утечки информации. Цифровые следы. Сбор информации из общедоступных источников. Приватность и анонимность.Федеральное и международное законодательство. Государственное регулирование и контроль в сфере защиты персональных данных. Основные определения. Операции с персональными данными. Обезличивание персональных данных. Категории персональных данных. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора персональных данных. Ответственность за нарушения для физических лиц и для организаций. Последствия реализации угроз. Порядок реагирования на нарушения. Защита от атак методами социальной инженерии. Классификация атак и их характеристики. Выявление признаков неправомерного воздействия на пользователей информационных систем. Криминально-психологические приемы злоумышленников. Формирование устойчивости к эмоционально-волевым методам и манипулированию сознанием.	Лекционные занятия	7	4	ОПК-7 ПК-2
2.8	Тема "Защита персональных данных в цифровой среде" Разработка и реализация политики защиты персональных данных в организациях. Особенности защиты персональных данных несовершеннолетних. Защита персональных данных в интернете вещей и смарт-устройствах. Перспективы и вызовы в области защиты персональных данныхЗащита от атак методами социальной инженерии. Системы обнаружения вторжений (IDS) для выявления подозрительной активности. Способы развития критического мышления для выявления подозрительных действий. Опыт разработки и реализации программы защиты от социальной инженерии.Международное сотрудничество в борьбе с социальной инженерией.	Самостоятельная работа	7	4	ОПК-7 ПК-2
2.9	Тема "Основы защиты коммерческой тайны " Правовые основы защиты коммерческой тайны. Сущность и содержание коммерческой тайны. Сведения, составляющие коммерческую тайну. Права обладателя коммерческой тайны. Практика защиты коммерческой тайны.	Лекционные занятия	7	2	ОПК-7 ПК-2
2.10	Тема "Основы защиты коммерческой тайны " Международное законодательство в области защиты коммерческой тайны. Этические и социальные аспекты защиты коммерческой тайны. Перспективные методы защиты коммерческой тайны.	Самостоятельная работа	7	6	ОПК-7 ПК-2
2.11	Практическое задание 3 Антивирусное ПО. Облачные антивирусы.Функциональные возможности и ограничения.VirusTotal.Hybrid Analysis. Kaspersky Threat Intelligence Portal.	Практические занятия	7	4	ОПК-7 ПК-2
2.12	Практическое задание 4 Социальная инженерия и разведка по общедоступным источникам. Инструменты поиска общедоступной информации. Исследование общедоступных источников.Сбор и анализ информации. Выявление фишинговых ресурсов.	Практические занятия	7	4	ОПК-7 ПК-2

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	Рогозин, В. Ю., Галушкин, И. Б., Новиков, В. К., Вепрев, С. Б.	Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017	ЭБС «IPR SMART»
2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	ЭБС «Университетская библиотека онлайн»
3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	ЭБС «IPR SMART»
4	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	ЭБС «IPR SMART»
5		Системный администратор: журнал	Москва: Положевец и партнеры, 2019	ЭБС «Университетская библиотека онлайн»
6	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	ЭБС «Университетская библиотека онлайн»
7	Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012	ЭБС «IPR SMART»
8	Сычев, Ю. Н.	Основы информационной безопасности: учебно -методический комплекс	Москва: Евразийский открытый институт, 2012	ЭБС «IPR SMART»
9	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014	ЭБС «IPR SMART»
10	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	ЭБС «IPR SMART»

5.2. Профессиональные базы данных и информационные справочные системы

Консультант+
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru
Профессиональная ИТ блог-платформа https://habr.com/
Цифровой журнал, посвящённый вопросам информационной безопасности https://xakep.ru/

5.3. Перечень программного обеспечения

Операционная система РЕД ОС
Libre Office
VirusTotal
Kaspersky Threat Intelligence Portal
Hybrid Analysis
VirtualBox
KaliLinux

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.

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
ОПК-7: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.			
З: подходы к самостоятельному поиску информации с использованием различных информационных ресурсов в области обеспечения личной и корпоративной кибербезопасности	отвечает на вопросы опроса и на вопросы на экзамене	полнота и содержательность ответа на экзамене, опросе, соответствие ответов материалу, изученному в рамках лекций, практических работ и самостоятельной работы	О (вопросы 1-60) Э (вопросы 1-45)
У: подбирать релевантные технологии обеспечения личной и корпоративной кибербезопасности для решения задач профессиональной деятельности.	выполняет лабораторные задания	соответствие результатов лабораторного задания запланированным, четко сформулированные выводы, уместные, полные и ясные ответы на вопросы и комментарии	ПЗ (практическое задание 1-4)
В: навыками применения методиками проведения анализа научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности с целью повышения уровня	выполняет лабораторные задания	соответствие представленных отчетов по вопросам обеспечения информационной безопасности требованиям действующих нормативных и методических	ПЗ (практическое задание 1-4)

самоорганизации и компетенций в области обеспечения личной и корпоративной кибербезопасности		документов в области информационной безопасности	
ПК-2: Способен использовать в профессиональной деятельности коммуникационные технологии, государственные и муниципальные информационные системы; осуществлять внутриорганизационные и межведомственные коммуникации необходимые для решения профессиональных задач			
З: способы решения стандартных задач профессиональной деятельности в области информационной безопасности на основе организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации с применением информационно-коммуникационных технологий	отвечает на вопросы опроса и на вопросы на экзамене	полнота и содержательность ответа на экзамене, опросе, соответствие ответов материалу, изученному в рамках лекций, практических работ и самостоятельной работы	О (вопросы 61-130) Э (вопросы 46-90)
У: использовать современные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе анализа требований нормативно-правовых актов в области обеспечения личной и корпоративной кибербезопасности	выполняет лабораторные задания	соответствие результатов лабораторного задания запланированным, четко сформулированные выводы, уместные, полные и ясные ответы на вопросы и комментарии	ПЗ (практическое задание 1-4)
В: навыками организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами контролирующих органов	выполняет практические задания	соответствие технологического процесса защиты информации требованиям нормативно-методических документов контролирующих органов и содержанию задачи в сфере	ПЗ (практическое задание 1-4)

		информационной безопасности	

О – опрос; ПЗ – практическое *задания; Э – вопросы к экзамену*

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

В разделе приводятся варианты оценочных средств: вопросы к экзамену, перечень вопросов для опроса, перечень лабораторных заданий.

.

Вопросы к зачету
по дисциплине Методы обеспечения кибербезопасности

1. Основные понятия в области информационной безопасности и кибербезопасности.
2. Модели информационной безопасности с примерами. Свойства целостности, доступности и конфиденциальности информации.
3. Направления защиты информации. Принципы защиты информации.
4. Пирамида безопасности. Пентагон моделирование угроз. Модель Защита – Обнаружение – Реагирование. Модель Треугольника угроз.
5. Принцип наименьшей привилегии. Принцип разделения обязанностей. Принцип экономической эффективности. Принцип усиления слабого звена. Принцип эшелонированности обороны.
6. Структура и содержание законодательства в области информационной безопасности.
7. Структура системы организационной защиты информации в РФ.
8. Классификация информации по режимам доступа.
9. Информация, доступ к которой не может быть ограничен.
10. Организация работы со сведениями, отнесенными к государственной тайне.
11. Перечень сведений конфиденциального характера.
12. Лицензирование деятельности в области защиты информации.
13. Сертификация средств защиты информации.
14. Роль информационной и кибербезопасности в обеспечении национальной безопасности личности, общества и государства.
15. Национальные интересы РФ в информационной сфере.
16. Защита критической информационной инфраструктуры.
17. Противодействие киберпреступности и кибертерроризму.
18. Обеспечение информационной безопасности государственных органов и организаций.
19. Источники и виды угроз. Модели классификации угроз.
20. Требования к структуре и содержанию моделей угроз. Модель нарушителя.
21. Нормативные и методические документы ФСТЭК в области моделирования угроз.
22. Технические каналы утечки информации.
23. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок,
24. Угрозы утечки акустической (речевой) информации.
25. Угрозы утечки видовой информации.
26. Инженерно-техническая защита информации.
27. Правовые методы защиты информации. Организационные методы защиты информации.
28. Программно- технические методы защиты информации.
29. Средства идентификации и аутентификации.
30. Управление доступом.
31. Антивирусное программное обеспечение.
32. Межсетевые экраны.
33. Системы обнаружения и предотвращения вторжений.
34. Средства резервирования.
35. Средства централизованного управления и контроля за состоянием информационной безопасности.
36. Средства выявления и предотвращения инсайдерских угроз и рисков утечки информации ограниченного доступа.
37. Искусственный интеллект в задачах обеспечения информационной безопасности.
38. Особенности и последствия реализации угроз на различных уровнях информационной инфраструктуры организации.

39. Подбор релевантных мер защиты на различных уровнях информационной инфраструктуры организации.
40. Организация процессов систематического мониторинга состояния кибербезопасности в организации.
41. Аудит безопасности и тестирование на проникновение.
42. Инструментарий форензики.
43. Основные понятия и принципы криптографии.
44. Правовое регулирование криптографических средств защиты информации.
45. Принципы функционирования симметричных криптосистем.
46. Основные симметричные криптоалгоритмы.
47. Принципы функционирования асимметричных криптосистем.
48. Основные асимметричные криптоалгоритмы.
49. Достоинства и недостатки симметричных и асимметричных криптосистем.
50. Назначение и принципы функционирования электронной подписи. Алгоритмы. Коллизии.
51. Криптостойкость. Классификация атак на криптосистемы.
52. Перспективные криптографические технологии и алгоритмы.
53. Квантовая криптография.
54. Компьютерная вирусология.
55. Классификация вредоносного ПО.
56. Последствия вирусных атак.
57. Особенности механизмов воздействия вредоносного ПО.
58. Выявление вредоносного ПО.
59. Антивирусные технологии и их практическое применение.
60. Развитие и эволюция вредоносного программного обеспечения.
61. Экономические аспекты и последствия атак вредоносного программного обеспечения.
62. Управление уязвимостями и патчинг программного обеспечения.
63. Классификация сетевых атак и их характеристика.
64. Последствия сетевых атак.
65. Способы обнаружения сетевых атак.
66. Способы защиты от сетевых атак.
67. Межсетевое экранирование.
68. Технология VPN.
69. Безопасность использования беспроводных сетей.
70. Уязвимости веб-приложений: инъекции, кросс-сайтовый скриптинг.
71. Уязвимости операционных систем и сервисов: эксплойты для получения доступа.
72. Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).
73. Использование облачных брандмауэров и антивирусов.
74. Журналирование и мониторинг сетевой активности.
75. Классификация атак методами социальной инженерии и их характеристики.
76. Выявление признаков неправомерного воздействия на пользователей информационных систем. Формирование устойчивости к эмоционально-волевым методам и манипулированию сознанием.
77. Международное сотрудничество в борьбе с социальной инженерией.
78. Источники угроз персональным данным и каналы утечки информации. Последствия реализации угроз в сфере персональных данных.
79. Цифровые следы.
80. Сбор информации из общедоступных источников.
81. Федеральное и международное законодательство в сфере защиты персональных данных. Государственное регулирование и контроль в сфере защиты персональных данных.
82. Операции с персональными данными. Обезличивание персональных данных.

83. Особенности обработки различных категорий персональных данных.
84. Класс защищенности информационной системе персональных данных.
85. Принципы и условия обработки персональных данных.
86. Права субъекта персональных данных. Обязанности оператора персональных данных. Ответственность за нарушения требований в сфере защиты персональных данных. Порядок реагирования на нарушения в сфере защиты персональных данных.
87. Защита персональных данных в интернете вещей и смарт-устройствах.
88. Сущность и содержание коммерческой тайны. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
89. Права обладателя коммерческой тайны. Обязанности лица, получившего доступ к коммерческой тайне.
90. Международное законодательство в области защиты коммерческой тайны.

Критерии оценивания*:*

Критерии оценивания:

- оценка «отлично» (84-100 баллов) выставляется, если изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- оценка хорошо» (67-83 баллов) – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, студент усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- оценка «удовлетворительно» (50-66 баллов) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- оценка неудовлетворительно» (0-49 баллов) ответы не связаны с вопросами*,* наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Перечень вопросов для опроса:

1. Основные понятия в области информационной безопасности и кибербезопасности.
2. Модели информационной безопасности с примерами.
3. Свойства целостности, доступности и конфиденциальности информации.
4. Направления защиты информации.
5. Принципы защиты информации.
6. Пирамида безопасности.
7. Пентагон моделирование угроз.
8. Модель Защита – Обнаружение – Реагирование.
9. Модель Треугольника угроз.
10. Принцип наименьшей привилегии.
11. Принцип разделения обязанностей.
12. Принцип экономической эффективности.
13. Принцип усиления слабого звена.

14. Принцип эшелонированности обороны.
15. Структура и содержание законодательства в области информационной безопасности.
16. Структура системы организационной защиты информации в РФ.
17. Контролирующие и регулирующие органы в сфере защиты информации.
18. Классификация информации по режимам доступа.
19. Информация, доступ к которой не может быть ограничен.
20. Нормативно-правовая база функционирования систем защиты информации.
21. Компьютерные преступления и особенности их расследования.
22. Организация работы со сведениями, отнесенными к государственной тайне.
23. Перечень сведений конфиденциального характера.
24. Лицензирование деятельности в области защиты информации.
25. Сертификация средств защиты информации.
26. Информационная безопасность личности, общества и государства.
27. Роль информационной и кибербезопасности в обеспечении национальной безопасности государства.
28. Национальные интересы РФ в информационной сфере.
29. Защита критической информационной инфраструктуры.
30. Противодействие киберпреступности и кибертерроризму.
31. Обеспечение информационной безопасности государственных органов и организаций.
32. Научно-техническое развитие в области информационной безопасности.
33. Источники и виды угроз.
34. Модели классификации угроз.
35. Модель угроз информационного ресурса.
36. Модель нарушителя.
37. Требования к структуре и содержанию моделей угроз.
38. Нормативные и методические документы ФСТЭК в области моделирования угроз.
39. Технические каналы утечки информации.
40. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок,
41. Угрозы утечки акустической (речевой) информации.
42. Угрозы утечки видовой информации.
43. Инженерно-техническая защита информации.
44. Правовые методы защиты информации.
45. Организационные методы защиты информации.
46. Программно- технические методы защиты информации.
47. Средства идентификации и аутентификации.
48. Управление доступом.
49. Антивирусное программное обеспечение.
50. Межсетевые экраны.
51. Средства резервирования.
52. Средства централизованного управления и контроля за состоянием информационной безопасности.
53. Средства выявления и предотвращения инсайдерских угроз и рисков утечки информации ограниченного доступа.
54. Искусственный интеллект в задачах обеспечения информационной безопасности.
55. Особенности реализации угроз на различных уровнях информационной инфраструктуры организации.
56. Последствия реализации угроз на различных уровнях информационной инфраструктуры организации.
57. Подбор релевантных мер защиты на различных уровнях информационной инфраструктуры организации.

58. Организация процессов систематического мониторинга состояния кибербезопасности в организации.
59. Аудит безопасности и тестирование на проникновение.
60. Инструментарий форензики.
61. Основные понятия и принципы криптографии.
62. Правовое регулирование криптографических средств защиты информации. Принципы функционирования симметричных криптосистем.
63. Функциональная схема взаимодействия участников симметричного криптографического обмена.
64. Основные симметричные криптоалгоритмы.
65. Принципы функционирования асимметричных криптосистем.
66. Функциональная схема взаимодействия участников асимметричного криптографического обмена.
67. Основные асимметричные криптоалгоритмы.
68. Достоинства и недостатки симметричных и асимметричных криптосистем.
69. Электронная подпись.
70. Коллизии электронной подписи.
71. Криптостойкость.
72. Классификация атак на криптосистемы.
73. Алгоритмы электронной подписи.
74. Перспективные криптографические технологии.
75. Квантовая криптография.
76. Компьютерная вирусология.
77. Классификация вредоносного ПО.
78. Последствия вирусных атак.
79. Особенности механизмов воздействия вредоносного ПО.
80. Выявление вредоносного ПО.
81. Антивирусные технологии и их практическое применение.
82. Развитие и эволюция вредоносного программного обеспечения.
83. Экономические аспекты и последствия атак вредоносного программного обеспечения.
84. Управление уязвимостями и патчинг программного обеспечения.
85. Классификация сетевых атак и их характеристика.
86. Последствия сетевых атак.
87. Способы обнаружения сетевых атак.
88. Способы защиты от сетевых атак.
89. Межсетевое экранирование.
90. Технология VPN.
91. Безопасность использования беспроводных сетей.
92. Уязвимости веб-приложений: инъекции, кросс-сайтовый скриптинг.
93. Уязвимости операционных систем и сервисов: эксплойты для получения доступа.
94. Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).
95. Использование облачных брандмауэров и антивирусов.
96. Журналирование и мониторинг сетевой активности.
97. Реагирование на инциденты: планы и процедуры.
98. Классификация атак методами социальной инженерии и их характеристики.
99. Выявление признаков неправомерного воздействия на пользователей информационных систем.
100. Формирование устойчивости к эмоционально-волевым методам и манипулированию сознанием.
101. Системы обнаружения вторжений (IDS) для выявления подозрительной активности.
102. Международное сотрудничество в борьбе с социальной инженерией.
103. Источники угроз персональным данным и каналы утечки информации.

104. Цифровые следы.
105. Сбор информации из общедоступных источников.
106. Приватность и анонимность
107. Федеральное и международное законодательство в сфере защиты персональных данных.
108. Государственное регулирование и контроль в сфере защиты персональных данных.
109. Операции с персональными данными.
110. Методы обезличивания персональных данных.
111. Категории персональных данных.
112. Класс защищенности информационной системе персональных данных.
113. Принципы и условия обработки персональных данных.
114. Права субъекта персональных данных.
115. Обязанности оператора персональных данных.
116. Ответственность за нарушения требований в сфере защиты персональных данных.
117. Последствия реализации угроз в сфере персональных данных.
118. Порядок реагирования на нарушения в сфере защиты персональных данных.
119. Разработка и реализация политики защиты персональных данных в организациях.
120. Особенности защиты персональных данных несовершеннолетних.
121. Защита персональных данных в интернете вещей и смарт-устройствах.
122. Перспективы и вызовы в области защиты персональных данных.
123. Правовые основы защиты коммерческой тайны.
124. Сущность и содержание коммерческой тайны. Сведения, составляющие коммерческую тайну.
125. Сведения, которые не могут составлять коммерческую тайну.
126. Права обладателя коммерческой тайны.
127. Программные средства для защиты коммерческой тайны.
128. Практика защиты коммерческой тайны.
129. Международное законодательство в области защиты коммерческой тайны.
130. Перспективные методы защиты коммерческой тайны.

Критерии оценивания*:*

Для каждого вопроса:

– 1 балл дан полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
– 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов за семестр – 20.

Практические задания

Раздел 1. Основы информационной безопасности и кибербезопасности

Практическое задание 1.
Защита информации в пакетах офисных программ.

Цель работы: Освоить основные функции безопасности в LibreOffice для защиты документов и данных.

Задачи:

1. Шифрование документа

- Запустите LibreOffice Writer.
- Создайте новый документ или откройте существующий.
- откройте диалог сохранения файла. Выберите имя файла, место для его сохранения. Отметьте пункт «Сохранить с паролем». После нажатия кнопки «Сохранить», появится окно настройки сохранения с шифрованием. Задайте пароль.
- Попробуйте ввести сначала неправильный пароль, а затем -правильный и проследите поведение программы во время этих действий. Попробуйте открыть файл в других доступных программах.
- Если развернуть пункт «Параметры», откроются дополнительные настройки защиты: возможность задать пароль, позволяющий редактировать содержимое документа, а также флажок «Открыть только для чтения».
- Исследуйте различные комбинации основных и дополнительных параметров и обязательно зафиксируйте в отчете результаты и выводы. Также проверьте, шифруется ли информация о свойствах файла.

2. Защита частей документа от изменений
   - LibreOffice поддерживает защиту от изменений отдельных фрагментов документа. Для этого необходимо, чтобы документ содержал разделы. Их можно создать с помощью команды «Вставка — Разделы». Можно сначала создать раздел и размещать в нём текст, а можно выделить уже готовую часть документа и превратить её в новый раздел.
   - Исследуйте, как работает функция защита от изменений с паролем и без, есть ли какая-то разница в реакции программы при этом. В каких сценариях это может быть полезно?

3. Защита пометок рецензирования
   - При каждом изменении документа функция рецензирования регистрирует, кто внес изменение. Эта функция может быть включена с защитой, чтобы её можно было выключить только при вводе правильного пароля. До отключения функции все изменения будут регистрироваться. Принять или отклонить изменения невозможно.

4. Защита врезок, графики и объектов OLE
   - Предусмотрена возможность защитить содержимое, положение и размеры вставленных графических объектов. Это относится также к врезкам (в модуле Writer) и к объектам OLE.
   - Чтобы защитить изображение выполните: Формат-Изображение-Свойства-Опции

5. Защита таблиц от изменений
   - Еще одна функция защиты от изменений применяется в таблицах в LibreOffice Writer. Создайте таблицу и поместите курсор в ячейку или выделите нужный диапазон ячеек.
   - Откройте контекстное меню и выбрать пункт «Ячейка —Защитить» или в главном меню выбрать «Таблица —Защита ячейки».
   - Исследуйте, как работает эта функция, в т.ч. как снимать защиту.

6. Защита листов от изменений в LibreOffice Calc

- Создайте или откройте документ LibreOffice Calc
- Включите защиту листа. Для этого нужно выбрать соответствующий пункт в контекстном меню листа.
- Исследуйте, как работает функция при различных комбинациях параметров.

7. Защита ячеек от изменений в LibreOffice Calc.

- Защита выбранных ячеек будет осуществляться только тогда, когда будет активна защита листа, на котором они расположены.
- Выберите ячейку или диапазон ячеек, которые хотите защитить. Вызовите контекстное меню правой кнопкой мыши и выберите пункт «Формат ячеек» (или в главном меню «Формат— Ячейки»). В появившемся окне перейдите на вкладку «Защита ячейки».
- Исследуйте, как работает функция в различных комбинациях параметров.

8. Шифрование документа LibreOffice Calc
   - Исследуйте, есть ли отличия в функционале шифрования документа между LibreOffice Calc и LibreOffice Writer.

Практическое задание 2.
Инструменты шифрования.

Краткая аннотация:

Шифрование на основе симметричных алгоритмов является одним из наиболее ранних способов защиты информации. В рамках лабораторного задания будет освоен один из наиболее распространённых шифров, дающий общее представление о технологии симметричного шифрования. В современных задачах защиты информации наиболее распространены программные средства защиты информации, реализующие ассиметричные алгоритмы шифрования. Одно из рас пространных средств – ПО Veracrypt.

Цель:

Познакомиться с алгоритмами симметричного шифрования и программными средствами, реализующими защиту информации с помощью ассиметричных алгоритмов в различных режимах.

Задачи:

- Изучение алгоритмов симметричного шифрования.
- Реализация простого шифра сдвига средствами LibreOffice.
- Изучение инструментов асимметричного шифрования.
- Практика применения ПО Veracrypt
- Генерация ключевой пары.
- Шифрование и расшифрование.

Раздел 2. Защита от угроз и конфиденциальность

Практическое задание 3
Антивирусное ПО

Краткая аннотация.

При отсутствии возможности проверить подозрительный файл, ссылку и т.п. антивирусом либо при недоверии к результативности работы установленного антивирусного ПО можно воспользоваться одним из бесплатных и общедоступных онлайн-антивирусов, например, продуктом от корпорации Google https://www.virustotal.com//

Сервис проверяет в режиме реального времени загруженный файл с помощью нескольких десятков антивирусов от различных производителей и позволяет пользователю сформировать консенсус-мнение.

Также существуют сервисы со схожим назначением, например: https://hybrid-analysis.com/, https://opentip.kaspersky.com/

Цель:

Познакомиться с функциональными возможностями антивирусных онлайн-сервисов и провести их сравнительный анализ.

Задачи:

1. Исследуйте и протестируйте возможности каждого сервиса и выделите наиболее важный на ваш взгляд функционал. В качестве подтверждения прикрепите в отчет скриншоты (не менее 5 на каждый сервис) с короткими комментариями к каждому.
2. Проанализируйте функционал, процесс взаимодействия пользователя с сервисами и полученные отчеты о сканировании. Выделите не менее 5 значимых на ваш взгляд критериев (желательно, измеримых) и проведите сравнительный анализ названных сервисов. Зафиксируйте результаты в отчете.
3. Будьте готовы продемонстрировать работу с каждым сервисом и подробно прокомментировать ее по требованию преподавателя.

Практическое задание 4.
Противодействие социальной инженерии и разведка по общедоступным источникам.

Краткая аннотация:

Социальная инженерия является одним из наиболее результативных и потому наиболее опасных видов атак, т.к. позволяет злоумышленникам обходить большинство средств программно-технической защиты информации. При подготовке атаки злоумышленники зачастую активно собирают информацию из общедоступных источников, в т.ч. содержащую персональные данные. В связи с этим для снижения вероятности реализации подобных атак важно понимать, какие источники данных могут быть использованы и каковы возможности инструментов.

Цель:

Лабораторное задание направлено на формирование осведомленности в области противодействия атакам социальной инженерии и защиты персональных данных.

Задачи:

- Инструменты поиска общедоступной информации.
- Исследование общедоступных источников.
- Сбор и анализ информации.
- Потенциальные угрозы применения общедоступной информации.
- Выявление фишинговых ресурсов.
- Формирование осведомленности в области защиты от атак методами социальной инженерии

Критерии оценивания*:*

15-20 баллов – задание выполнено верно и в полном объеме, обучающийся подробно комментирует ход выполнения и результаты;

10-14 баллов – при выполнении задания были допущены неточности, не влияющие на результат, обучающийся подробно комментирует ход выполнения и результаты;

5-9 баллов – при выполнении задания были допущены ошибки, обучающийся комментирует ход выполнения и результаты;

1-4 балла – при выполнении задания были допущены существенные ошибки, обучающийся допускает существенные неточности при комментировании хода выполнения и результатов;

0 баллов – задание не выполнено.

20 баллов максимально за 1 практическое задание.

Максимальное количество баллов за семестр – 80.

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 экзамена.

Экзамен проводится по окончанию теоретического обучения в соответствии с расписанием. Количество вопросов в задании – 3. Объявление результатов производится в день экзамена. Результаты аттестации заносятся в электронную 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 подготовке 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 лабораторной 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. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом опроса. 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.