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.
«28» 08 2023 г.

Рабочая программа дисциплины

Информационная безопасность

Направление

01.03.05 «Статистика»

Направленность

01.03.05.01 «Анализ больших данных»

Для набора 2020 года

Квалификация
Бакалавр

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	152	152	152	152
Часы на контроль	36	36	36	36
Итого	252	252	252	252

ОСНОВАНИЕ

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

Программу составил(и): доцент, Назарян С.А. _____, к.т.н., доцент, Серпенинов О.В. _____

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

Методическим советом направления: к.э.н., доцент, Кислая И.А. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний в области информационной безопасности и защиты информации по организационно- правовой защите коммерческой, служебной, профессиональной тайны, персональных данных; формирование умений и практических навыков по правовому, организационному и техническому обеспечению защиты информации при решении задач профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОК-7: способностью к самоорганизации и самообразованию

ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-11:способностью обеспечивать сохранность и конфиденциальность индивидуальных данных и другой статистической информации

В результате освоения дисциплины обучающийся должен:

Знать:

- подходы к самостоятельному поиску информации с использованием различных информационных ресурсов в области информационной безопасности
- 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
- цели, задачи, инструменты и процессы системы защиты конфиденциальной информации

Уметь:

- использовать технологии дистационного образования, поиска теоретической и практико-ориентированной информации в области информационной безопасности и защиты информации
- использовать современные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе анализа требований нормативно-правовых актов в области информационной безопасности
- анализировать эффективность систем защиты информации и определять направления ее совершенствования при обеспечении сохранности и конфиденциальности информации

Владеть:

- методиками 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 информационной безопасности и защиты информации
- методологией по разработке комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты на основе анализа нормативно-правовых актов в области информационной безопасности при решении задач профессиональной деятельности
- способами организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами контролирующих органов

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Основы информационной безопасности				
1.1	Тема 1.1 "Введение в информационную безопасность" Понятийный аппарат в области информационной безопасности и кибербезопасности. Модели информационной безопасности. Целостность, доступность и конфиденциальность. Принципы и направления защиты информации. /Лек/	7	2	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.2	Тема 1.1 "Введение в информационную безопасность" 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. /Ср/	7	10	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7

1.3	Тема 1.2 "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. /Лек/	7	2	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.4	Тема 1.2 "Правовые основы обеспечения информационной безопасности" Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования. Организация работы со сведениями, отнесенными к государственной тайне. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации. /Ср/	7	14	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.5	Тема 1.3 "Информационная безопасность личности, общества и государства" Информационная безопасность личности, общества и государства в условиях цифровой экономики. Роль информационной и кибербезопасности в обеспечении национальной безопасности государства. Национальные интересы РФ в информационной сфере. Защита критической информационной инфраструктуры. /Лек/	7	2	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.6	Тема 1.3 "Информационная безопасность личности, общества и государства". Противодействие киберпреступности и кибертерроризму.Обеспечение информационной безопасности государственных органов и организаций. Научно-техническое развитие в области информационной безопасности. /Ср/	7	12	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.7	Тема 1.4 "Классификация угроз информационной безопасности " Источники и виды угроз. Модели классификации угроз. Модель угроз информационного ресурса. Модель нарушителя. /Лек/	7	2	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.8	Тема 1.4 "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. /Ср/	7	12	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.9	Тема 1.5 "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. /Лек/	7	2	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.10	Тема 1.5 "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. /Ср/	7	12	ОПК-1 ОК- 7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7

1.11	Тема 1.6 "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. /Лек/	7	2	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
1.12	Тема 1.6 "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 кибериндидентов. /Ср/	7	12	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1
1.13	Лабораторное задание 1 Защита информации в пакетах офисных программ LibreOffice. Управление доступом. Защита отдельных объектов содержимого от модификации и удаления. Шифрование. Электронная подпись. /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
1.14	Лабораторное задание 2 Развертывание лабораторного стенда для аудита безопасности информационной системы. Гипервизор VirtualBox /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
1.15	Лабораторное задание 3 Инструменты шифрования Изучение инструментов асимметричного шифрования. Генерация ключевой пары. Шифрование и расшифрование. /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
	Раздел 2. Защита от угроз и конфиденциальность				
2.1	Тема 2.1 "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. /Лек/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3
2.2	Тема 2.1 "Методы и средства криптографический защиты информации" Классификация атак на криптосистемы. Алгоритмы электронной подписи. Перспективные технологии. Квантовая криптография. /Ср/	7	20	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3
2.3	Тема 2.2 "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. /Лек/	7	2	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3
2.4	Тема 2.2 "Вредоносное программное обеспечение и способы защиты" Развитие и эволюция вредоносного программного обеспечения. Мотивация злоумышленника при использовании вредоносного программного обеспечения. Экономические аспекты и последствия атак вредоносного программного обеспечения. Управление уязвимостями и патчинг программного обеспечения. /Ср/	7	10	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3

2.5	Тема 2.3 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. /Лек/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3
2.6	Тема 2.3 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.Журиалирование и мониторинг сетевой активности.Реагирование на инциденты: планы и процедуры. /Ср/	7	20	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.3
2.7	Тема 2.4 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. /Лек/	7	2	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.8	Тема 2.4 Защита 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. /Ср/	7	10	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.9	Тема 2.5 "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. /Лек/	7	6	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.10	Тема 2.5 "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 данных /Ср/	7	10	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.11	Тема 2.6 "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. /Лек/	7	2	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.12	Тема 2.6 "Основы защиты коммерческой тайны " Международное законодательство в области защиты коммерческой тайны. Этические и социальные аспекты защиты коммерческой тайны. Перспективные методы защиты коммерческой тайны. /Ср/	7	10	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3
2.13	Лабораторное задание 4 Антивирусное ПО. Облачные антивирусы.Функциональные возможности и ограничения.VirusTotal.Hybrid Analysis. Kaspersky Threat Intelligence Portal. /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.1 Л2.3

2.14	Лабораторное задание 5. Исследование сетевой инфраструктуры. Портовое сканирование (TCP, UDP). Определение активных хостов. Определение операционной системы.Сканирование локальной сети. Сканирование удаленного хоста.Анализ результатов сканирования.Поиск уязвимостей.NMAP /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.3 Л1.2Л2.1 Л2.7 Л2.6 Л2.5 Л2.4 Л2.3 Л2.2
2.15	Лабораторное задание 6. Анализ сетевого трафика и обнаружению аномалий в сети. Захват сетевого трафика. Анализ трафика. Интерпретация пакетов.Обнаружение аномалий. Анализ результатов. Wireshark /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.3 Л1.2Л2.1 Л2.7 Л2.6 Л2.5 Л2.4 Л2.3 Л2.2
2.16	Лабораторное задание 7 Социальная инженерия и разведка по общедоступным источникам. Инструменты поиска общедоступной информации. Исследование общедоступных источников.Сбор и анализ информации. Выявление фишинговых ресурсов. KaliLinux /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.3 Л1.2Л2.1 Л2.7 Л2.6 Л2.5 Л2.4 Л2.3 Л2.2
2.17	Лабораторное задание 8 Аудит безопасности операционной системы инструментами тестирования на проникновение Исследование сетевой инфраструктуры. Поиск и выявление уязвимостей. Эксплуатация уязвимостей. Меры по защите.Kali Linux /Лаб/	7	4	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.3 Л1.2Л2.1 Л2.7 Л2.6 Л2.5 Л2.4 Л2.3 Л2.2
2.18	Экзамен /Экзамен/	7	36	ОПК-1 ОК-7 ПК-11	Л1.1 Л1.3 Л1.2Л2.1 Л2.7 Л2.6 Л2.5 Л2.4 Л2.3 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, составители	Заглавие	Издательство, год	Колич-во
Л1.1	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
Л1.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.3	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

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	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	http://www.iprbookshop.ru/72444.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2	Артемов, А. В.	Информационная безопасность: курс лекций	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014	https://www.iprbookshop.ru/33430.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Сычев, Ю. Н.	Основы информационной безопасности: учебно-методический комплекс	Москва: Евразийский открытый институт, 2012	https://www.iprbookshop.ru/14642.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012	https://www.iprbookshop.ru/10677.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	https://biblioclub.ru/index.php?page=book&id=576726 неограниченный доступ для зарегистрированных пользователей
Л2.6		Системный администратор: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562450 неограниченный доступ для зарегистрированных пользователей
Л2.7	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей

5.3 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/

5.4. Перечень программного обеспечения

Libre Office

Wireshark

NMAP

VirusTotal

Kaspersky Threat Intelligence Portal

Hybrid Analysis

VirtualBox

KaliLinux

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)

Помещение 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 проводится 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
ОК-7: способностью к самоорганизации и самообразованию			
З: подходы к самостоятельному поиску информации с использованием различных информационных ресурсов в области информационной безопасности	отвечает на вопросы опроса и на вопросы на экзамене	полнота и содержательность ответа на экзамене, опросе, соответствие ответов материалу, изученному в рамках лекций, лабораторных работ и самостоятельной работы	О (вопросы 1-40) Э (вопросы 1-27)
У: использовать технологии дистационного образования, поиска теоретической и практико-ориентированной информации в области информационной безопасности и защиты информации	выполняет лабораторные задания	соответствие результатов лабораторного задания запланированным, четко сформулированные выводы, уместные, полные и ясные ответы на вопросы и комментарии	ЛЗ (лабораторное задание 1-8)
В: методиками проведения анализа научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности с целью повышения уровня самоорганизации и	выполняет лабораторные задания	соответствие представленных отчетов по вопросам обеспечения информационной безопасности требованиям действующих нормативных и методических документов в	ЛЗ (лабораторное задание 1-8)
компетенций в области информационной безопасности и защиты информации		области информационной безопасности	
ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
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, лабораторных работ и самостоятельной работы	О (вопросы 41-78) Э (вопросы 31-55)
У: использовать современные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе анализа требований нормативно-правовых актов в области информационной безопасности	выполняет лабораторные задания	соответствие результатов лабораторного задания запланированным, четко сформулированные выводы, уместные, полные и ясные ответы на вопросы и комментарии	ЛЗ (лабораторное задание 1-8)
В: методологией по разработке комплекса организационно-технических мер по обеспечению информационной безопасности объекта защиты на основе анализа нормативно-правовых актов в области информационной безопасности при решении задач профессиональной деятельности;	выполняет лабораторные задания	соответствие технологического процесса защиты информации требованиям нормативно-методических документов контролирующих органов и содержанию задачи в сфере информационной безопасности	ЛЗ (лабораторное задание 1-8)

ПК-11: способностью обеспечивать сохранность и конфиденциальность индивидуальных данных и другой статистической информации			
З: цели, задачи, инструменты и процессы системы защиты конфиденциальной информации	отвечает на вопросы опроса и на вопросы на экзамене	полнота и содержательность ответа на экзамене, опросе, соответствие ответов материалу, изученному в рамках лекций, лабораторных работ и самостоятельной работы	О (вопросы 79-130,) Э (вопросы 1-90)
У: анализировать эффективность систем защиты информации и определять направления ее совершенствования при обеспечении сохранности и конфиденциальности информации.	выполняет лабораторные задания	соответствие результатов лабораторного задания запланированным, четко сформулированные выводы, уместные, полные и ясные ответы на вопросы и комментарии	ЛЗ (лабораторное задание 1-8)
В: способами организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами контролирующих органов	выполняет лабораторные задания	соответствие технологического процесса защиты информации требованиям нормативно-методических документов контролирующих органов и содержанию задачи в сфере информационной безопасности	ЛЗ (лабораторное задание 1-8)

О – опрос; ЛЗ – лабораторные 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 экзамену
по дисциплине Информационная безопасность

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.

Экзаменационный билет состоит из 2 теоретических вопросов и одного практико-ориентированного задания из перечня лабораторных заданий (лабораторные задания 1,4) для текущей аттестации.

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.

Лабораторные задания

Раздел 1. Основы информационной безопасности

Лабораторное 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.

Лабораторное задание 2.
Развертывание лабораторного стенда для аудита безопасности информационной системы

Краткая аннотация:
Kali Linux является специализированным Linux дистрибутивом для проведения тестирования на проникновение и аудита безопасности. Дистрибутив включает в себя более 300 программ для решения вопросов, связанных с исследованием безопасности различных информационных систем.

Цель:
Подготовить лабораторный стенд для проведения аудита безопасности с помощью дистрибутива Kali Linux

Задачи:

1. Подготовка лабораторного стенда

- Необходимо подготовить лабораторный стенд для проведения исследований безопасности объектов локальной сети с помощью дистрибутива ОС Linux Kali.

Для этого необходимо развернуть 2 виртуальные машины с помощью гипервизора Oracle VM VirtualBox и создать между ними локальную сеть.

- Запустите Oracle VM VirtualBox
- Создайте виртуальную машину (далее по тексту – ВМ) с именем Kali Linux. Т.к. в основе данного дистрибутива используется Debian 64-bit, то укажите соответствующий тип ОС.
- Объем ОЗУ задайте равным 1536 МБ.
- При создании виртуального жесткого диска укажите его емкость 20 Гб. Прочие параметры оставьте без изменения и завершите создание ВМ.
- Найдите на сетевом диске образ Kali Linux в папке, указанной преподавателем и скопируйте его на локальный диск.
- Подключите образ в качестве носителя к созданной виртуальной машине.
- Запустите виртуальную машину для начала установки.
- Выберите вариант Graphical Install.
- Выберите язык Russian и подтвердите свой выбор в следующем окне.
- Укажите раскладку клавиатуры «Английская американская».
- На этапе разметки дисков выберите метод «Авто – использовать весь диск».
- Завершите разметку диска, записав изменения на диск.
- На этапе настройки менеджера пакетов при запросе необходимости использования зеркала архивов из сети выберите «Нет».
- На следующем этапе инсталлятор ОС запросит установку загрузчика операционной системы, который называется GRUB. Выберите «Да».
- Завершите установку ОС Kali Linux и перезагрузите виртуальную машину.
- Завершите работу ОС.
- Создайте виртуальную машину с именем XP-Victim и установите на нее 32-х битную ОС Microsoft Windows XP Professional. Используйте образ, указанный преподавателем. Задайте для XP объем ОЗУ 512Мб. В последствии, при необходимости (в случае нестабильной работы) объем можно уменьшить до 256Мб.
- Для всех ВМ задайте тип сетевого подключения «Внутренняя сеть».
- Для Kali задайте IP 192.168.0.1, для XP 192.168.0.2.

2. Знакомство с интерфейсом Kali Linux

- После успешной загрузки рабочего стола Kali Linux ознакомьтесь с основными элементами интерфейса. Так, в левой части экрана находится панель «Избранное». Большинство приложений Kali Linux доступны из меню «Приложения» и сгруппированы по классификационным признакам назначения и порядка применения.
- ПО группы 01 – Information Gathering используется для сбора данных о целевой сети либо устройствах, позволяя установить состав сети, используемые порты и протоколы, версию ОС и сетевых служб и т.д.
- ПО группы 02 – Vulnerability Analysis используется после сбора данных для оценки потенциальных уязвимостей. ПО группы 03 Web Application Analysis используются для аудита безопасности веб-приложений. Также в этой группе представлены некоторые другие сетевые инструменты, например, веб-прокси.
- 04 Database Assessment применяется для проведения анализа безопасности основных СУБД, включая MSSQL, MySQL, and Oracle.
- Группа 05 Password Attacks представлена широким перечнем ПО для совершения парольных атак, включая подбор или вычисление паролей. С помощью приложений в группе

- 06 Wireless Attacks возможно проведение аудита безопасности беспроводных соединений, включая Wi-Fi, Bluetooth, RFID. Многие из представленных инструментов требуют наличия дополнительного оборудования.
- 07 Reverse Engineering содержит инструменты для анализа ПО, включая вредоносное.
- 08 Exploitation Tools - инструменты группы применяются для эксплуатации уязвимостей и непосредственно получения контроля над атакуемой информационной системой.
- 09 Sniffing & Spoofing применяются для перехвата сетевого траффика и манипуляции с сетевыми пакетами, включая их подмену.
- 10 Post Exploitation – инструменты позволяют закрепиться в атакуемой системе для дальнейшего упрощенного доступа к ней в нужное время.
- 11 Forensics используется для расследования инцидентов информационной безопасности
- 12 Reporting Tools используется для разработки и отправки отчетов о проведенном исследовании безопасности системы.
- 13 Social Engineeriing Tools – применяется для имитации атак социальной инженерией, включая фишинг.
- 14 System Services содержит перечень системных служб и сервисов, обеспечивающих работу специализированного ПО.

3. Подготовьте отчет по лабораторному заданию. Будьте готовы прокомментировать по требованию преподавателю ход выполнения и полученные результаты.

Лабораторное задание 3.
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

Лабораторное задание 4
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.

Лабораторное задание 5.
Исследование сетевой инфраструктуры

Краткая аннотация.

Инструмент NMAP позволяет обнаруживать активные узлы, определять открытые порты, выявлять уязвимости

Цель:

Познакомиться с методами сканирования сети с использованием Nmap, провести анализ активных узлов и выявление уязвимостей в сетевой инфраструктуре.

Задачи:

1. Сканирование активных узлов:
   - Откройте командную строку (терминал).

- Введите следующую команду для сканирования активных узлов в вашей сети: `nmap -sn <IP-диапазон>`
- Проанализируйте результаты, найденные активные узлы.

*Например, п*ри использовании команды `nmap -sn 192.168.1.0/24` будет осуществлено сканирование всех узлов в диапазоне IP-адресов от 192.168.1.1 до 192.168.1.254."

2. Сканирование открытых портов:

- Выберите один из найденных активных узлов.
- Введите команду `nmap -p- <IP-адрес>` для сканирования всех портов на выбранном узле.
- Проанализируйте результаты, обратите внимание на открытые порты и связанные с ними службы. Соберите информацию об этих сервисах – назначение, особенности функционирования, возможные угрозы и эксплойты

4. Определение операционной системы:

- Введите команду `nmap -O <IP-адрес>` для определения операционной системы выбранного узла.
- Проанализируйте полученные результаты и выявленную операционную систему.

5. Сканирование на уязвимости:

- Введите команду `nmap -sV --script vuln <IP-адрес>` для сканирования уязвимостей на выбранном узле.
- Проанализируйте результаты, обратите внимание на найденные уязвимости и связанные с ними скрипты.

6. Анализ результатов сканирования и уязвимостей:

- Изучите результаты сканирования активных узлов, определения открытых портов и наличия уязвимостей.
- Оцените, какие узлы и службы представляют наибольший потенциал для атак.

7. Сложное сканирование сети:

- Изучите возможности сканирования "в глубину" с помощью команды `nmap -A <IP-адрес>`.
- Проанализируйте полученные результаты, включая информацию о версиях служб и дополнительные данные.

8. Сканирование на уязвимости с Nmap NSE-скриптами:

- Ознакомьтесь с каталогом NSE-скриптов, доступных в Nmap, на официальном сайте.
- Выберите конкретные скрипты для детального сканирования уязвимостей.
- Введите команду с указанием выбранных скриптов: `nmap -p- --script <скрипты> <IP-адрес>`.

10. Интерпретация результатов:

- Обобщите все результаты сканирования и анализа уязвимостей.
- Составьте подробный отчет, описывающий ход выполнения работы, выявленные уязвимости, операционные системы и предлагаемые меры по устранению уязвимостей.

Лабораторное задание 6.
Анализ сетевого трафика и обнаружению аномалий в сети

Краткая аннотация:

Wireshark – это мощный инструмент для анализа сетевого трафика, который позволяет перехватывать и анализировать данные, передаваемые по сети. В данной лабораторной работе вы ознакомитесь с основами использования Wireshark для анализа пакетов, понимания основ сетевого взаимодействия и выявления проблем и наглядно увидите разницу между различными протоколами передачи данных.

Цель:

Познакомиться с инструментом анализа сетевого трафика Wireshark, освоить базовые навыки его использования для мониторинга и анализа сетевой активности, а также развить понимание основных протоколов и взаимодействий в компьютерных сетях.

Задачи:

1. Захват сетевого трафика:

- При запуске Wireshark, выберите сетевой интерфейс, который вы хотите мониторить.
- Ознакомьтесь с интерфейсом
- Нажмите кнопку "Start" или "Capture" (Захват), чтобы начать захват пакетов.

2. Анализ пакетов:

- В окне Wireshark появится список захваченных пакетов. Каждая строка представляет один пакет.
- Для детального анализа, разверните пакет, нажав на него дважды левой кнопкой мыши.
- Изучите различные поля пакета, такие как исходный и целевой IP-адреса, порты, протоколы и другие детали.

3. Фильтрация пакетов:

- Wireshark позволяет фильтровать пакеты по различным параметрам. Введите "ip.addr == ваш_IP" в поле фильтрации, чтобы отобразить только пакеты, связанные с вашим компьютером.
- Исследуйте различные виды фильтров и их использование для точного анализа интересующего вас трафика.

4. Анализ HTTP-трафика:

- Откройте веб-браузер и посетите какой-либо веб-сайт, функционирующий по протоколу HTTP (для подбора такого сайта можно использовать оператор поиска в поиске Google `поисковая фраза-inurl:https`)
- Вернитесь в Wireshark, остановите захвата и найдите пакеты с протоколом HTTP (используйте для этого фильтр со значением http).
- Выберите первый пакет в списке, это будет запрос к сайту, который вы посетили. Нажмите на него правой кнопкой мыши и выберите "Follow" > "TCP Stream". Откроется новое окно с деталями HTTP-сообщения.
- В этом окне вы увидите заголовки и содержимое запроса к серверу. Ознакомьтесь с информацией, такой как "Host" (адрес сайта), "User-Agent" (браузер) и другие заголовки запроса.
- Закройте окно с TCP Stream и выберите следующий пакет – это будет ответ от сервера на ваш запрос. Снова нажмите правой кнопкой мыши и выберите "Follow" > "TCP Stream". Теперь вы увидите детали HTTP-ответа.
- Проанализируйте структуру ответа, включая статус-код, заголовки и содержимое.
- Повторите действия для http сайтов, использующих форму ввода логина и пароля. Используйте фильтр `http.request.method == "POST"`, чтобы найти целевые пакеты с отправленными данными.
- Продолжайте изучать другие пакеты с протоколом HTTP, чтобы понять, какие данные обмениваются между браузером и сервером.

5. Анализ HTTPS-трафика:

- В современных сетях HTTPS широко используется для защиты данных. Запустите захват пакетов в Wireshark и посетите https://www.example.com или другой сайт с HTTPS.
- В Wireshark найдите пакеты с протоколом TLS.
- Обратите внимание, что HTTPS-трафик зашифрован, поэтому содержимое пакетов не будет видно в текстовом виде. Однако вы сможете анализировать метаданные и основные характеристики. Обязательно прокомментируйте в отчете, какие именно данные удалось выяснить.

6. Анализ DNS-трафика:

- DNS (Domain Name System) отвечает за преобразование доменных имен в IP-адреса.
- Найдите DNS-запросы и ответы в захваченном трафике.

7. Сохранение результатов:

- Вы можете сохранить захваченный трафик в файл для дальнейшего анализа.
- Выберите "File" > "Save" и выберите формат файла (например, pcap).

8. Интерпретация результатов:

- Обобщите все результаты захвата и анализа трафика.
- Составьте подробный отчет, описывающий ход выполнения работы, сделайте подробный вывод по каждому действию. Сделайте вывод о потенциальных уязвимостях, обнаруженных в ходе исследования.
- Будьте готовы продемонстрировать работу с программой и подробно прокомментировать ее по требованию преподавателя.

Лабораторное задание 7.
Социальная инженерия 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

Лабораторное задание 8.
Аудит безопасности операционной системы инструментами тестирования на проникновение

Краткая аннотация:

В состав Kali Linux входит инструмент Metasploit Framework, позволяющий проводить аудит безопасности путем тестирования на проникновения. В лабораторном задании требуется определить уязвимости целевой виртуальной машины, проэксплуатировать их и предложить меры по устранению уязвимости.

Цель:

Познакомиться с инструментарием Metasploit Framework

Задачи:

1. Исследование топологии сети и сбор данных об объектах сети с помощью ПО Network Mapper.

- Методология тестирования на проникновение подразумевает, что первым этапом является сбор информации о тестируемой системе.
- С помощью NMAP, предустановленного в Kali Linux соберите данные о ВМ, аудит которой проводится, включая открытые порты, службы и версию операционной системы.

2. Запуск Metasploit Framework

- В Kali Linux откройте новый терминал.
- Т.к. Metasploit Framework использует СУБД PostgreSQL, то сначала необходимо запустить соответствующую службу с помощью команды «**service postgresql start**».
- Для запуска Metasploit Framework кликните на соответствующую иконку в панели избранного. В результате будет создана БД и запущены все сопутствующие сервисы, обеспечивающие работу Metasploit Framework.

3.Получение контроля над целевой ВМ

- На следующем этапе предполагается поиск уязвимостей, которые могут использоваться для совершения атаки. Однако в данном случае предлагается использовать конкретную уязвимость, характерную для ОС Windows XP и позволяющую полностью удаленно контролировать атакуемый компьютер, выполняя произвольный код. Данная уязвимость называется «dcom». Введите в терминале команду «**search dcom**», которая позволит найти все эксплойты в БД, которые могут использовать данную уязвимость.
- Определите из перечня эксплойт с наивысшим рангом («great»). В представленном примере этот эксплойт имеет обозначение MS03-026. Для его запуска выполните команду «**use exploit/windows/dcerpc/ms03_026_dcom**».
- Для настройки параметров эксплойта выполните команду «**show options**».
- Задайте целевой IP адрес введя в терминале Metasploit Framework команду «set RHOST 192.168.0.2» и подставив необходимый IP адрес.
- Далее задаётся параметр payload. Необходимо отметить, что payload (дословно с англ. – полезная нагрузка) – это программный код, который выполняется после проведения успешной атаки. Таким образом exploit является способом эксплуатации уязвимости, способом получения доступа к системе, а payload – способом воздействия на систему, к которой уже получен доступ. Чтобы посмотреть список доступных эксплойтов выполните команду «show PAYLOADS».
  Затем выполните команду «**set PAYLOAD windows/shell_bind_tcp**». Эта команда позволит использовать эксплойт, дающий управление над тестируемой ВМ посредством командной строки.
- Убедитесь в том, что изменения в параметры были внесены корректно. Для этого вновь введите команду «**show options**». Напротив каждого параметра должно отображаться установленное значение.
- Запустите эксплойт на выполнение командой «**exploit**». В результате будет получен доступ к командной строке целевой ВМ.
- Теперь используя команду «**cd..**» перейдите в корневой каталог диска C: целевой ВМ.
- С помощью команды «**mkdir hacked**» создайте в корневом каталоге диска папку «hacked».
- Убедитесь в успешном создании каталога с помощью команды «dir».
- Для завершения работы с удаленным компьютером нажмите на клавиатуре сочетание Ctrl-C и подтвердите решение о завершении сессии.
- Для выгрузки эксплойта наберите команду «back».

4.Завершение

- Пользуясь ресурсами сети Интернет найдите патч от Microsoft, позволяющий ликвидировать описанную уязвимость.

- Составьте подробный отчет о ходе и результатах выполнения лабораторного задания

Критерии оценивания:

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

7-9 баллов – при выполнении задания были допущены неточности, не влияющие на результат, обучающийся подробно комментирует ход выполнения и результаты;

3-6 баллов – при выполнении задания были допущены ошибки, обучающийся комментирует ход выполнения и результаты;

1-2 балла – при выполнении задания были допущены существенные ошибки, обучающийся допускает существенные неточности при комментировании хода выполнения и результатов;

0 баллов – задание не выполнено.

10 баллов максимально за 1 лабораторное 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 расписанию промежуточной аттестации. Количество вопросов в задании – 2 теоретических вопроса и одно практико-ориентированного задания из перечня лабораторных заданий (лабораторные задания 1,4) для текущей аттестации. Объявление результатов производится в день экзамена. 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 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 лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы.

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

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