МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета_____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Операции и атаки в информационных системах и сетях»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____/Разинкин К.А./

Заведующий кафедрой Систем информационной безопасности _____/Остапенко А.Г./

Руководитель ОПОП _____/ Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является приобретение студентами знаний о структуре действий, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

1.2. Задачи освоения дисциплины

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области формализация описания информационных конфликтов социотехнических систем, стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах. Стратегии реализации информационных операций и атак;
- предоставить возможность изучения технологии поиска и анализа следов информационных операций и атак и инцидентов, прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Операции и атаки в информационных системах и сетях» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Операции и атаки в информационных системах и сетях» направлен на формирование следующих компетенций:

ПК-7.3 - Способен участвовать в проведении криминалистического анализа автоматизированных систем

ПК-7.2 - Способен разрабатывать проектные решения по защите информации в автоматизированных системах

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.3	знать технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов с том числе связанных с операциями и атаками в информационных системах и сетях
	уметь применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений

ПК-7.2	знать проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне
	уметь осуществлять разработку предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах с учётом знаний проблем и перспектив применения кибернетического оружия в современной сетецентрической войне

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Операции и атаки в информационных системах и сетях» составляет 16 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	216	108	108
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	144	72	72
Самостоятельная работа	288	144	144
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+
Общая трудоемкость: академические часы зач.ед.	 576 16	 288 8	 288 8

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение. Классификация атак	Классификация по характеру воздействия; по цели воздействия; по наличию обратной связи с атакуемым объектом; по условию начала осуществления воздействия; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Примеры.	12	24	48	84
2	Этапы реализации атак	сбор информации: изучение окружения; идентификация топологии сети; идентификация узлов; идентификация сервисов и сканирование портов;	12	24	48	84

		идентификация операционной системы; определение роли узла; определение уязвимостей узла; реализация атаки; проникновение; установление контроля; завершение атаки				
3	Краткое описание некоторых сетевых атак	фрагментация данных; атака Ping flooding; нестандартные протоколы, инкапсулированные в IP;атака smurf; атака DNS spoofing; атака IP spoofing; навязывание пакетов; Sniffing — прослушивание канала; перехват пакетов на маршрутизаторе; навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки):SYN-flood,UDP-flood	12	24	48	84
4	Технологии обнаружения атак	методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети	12	24	48	84
5	Социальная инженерия	Популярные фишинговые схемы: несуществующие ссылки; мошенничество с использованием брендов известных корпораций; подложные лотереи; ложные антивирусы и программы для обеспечения безопасности; IVR или телефонный фишинг. Сбор информации из открытых источников: плечевой серфинг; обратная социальная инженерия Способы защиты от социальной инженерии. Классификация угроз: угрозы, связанные с телефоном; угрозы, связанные с электронной почтой; угрозы, связанные с использованием службы мгновенного обмена сообщениями. Основные защитные методы	12	24	48	84
6	Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне	Концепция «сетецентрических войн». Наступательные операции в киберпространстве как составная часть информационной войны. Наступательные операции против АСУ инфраструктурных и технологических объектов. Оборонительные операции как часть мер по обеспечению информационной безопасности в мирное время. Перспективы развития концепции кибернетических операций	12	24	48	84
		Итого	**72**	**144**	**288**	**504**

5.2 Перечень лабораторных работ

1.Оценка степени поражения информационным оружием при мониторинге сетевого пространства на предмет выявления информационных операций.

2.Оценка эффективности перепрограммирования субъектов информационного воздействия при мониторинге сетевого пространства на предмет выявления информационных операций.

3.Математическая модель распространения слухов и понятие «реальное время» информационной операции.

4. Формальная постановка задачи на формирование плана информационной операции

5. Планирование информационной операции
6. Моделирование информационной операции

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-7.3	знать технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов с том числе связанных с операциями и атаками в информационных системах и сетях	знание технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов с том числе связанных с операциями и атаками в информационных системах и сетях	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений	умение применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-7.2	знать проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне	знание проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять разработку предложений по	умение осуществлять разработку предложений по совершенствованию	Выполнение работ в срок, предусмотренный в рабочих	Невыполнение работ в срок, предусмотренный в рабочих

	совершенствованию системы управления безопасностью информации в автоматизированных системах с учётом знаний проблем и перспектив применения кибернетического оружия в современной сетецентрической войне	системы управления безопасностью информации в автоматизированных системах с учётом знаний проблем и перспектив применения кибернетического оружия в современной сетецентрической войне	программах	программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-7.3	знать технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов с том числе связанных с операциями и атаками в информационных системах и сетях	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-7.2	знать проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь осуществлять разработку предложений по совершенствованию	Решение стандартных практических задач	Задачи решены в полном объеме и	Продемонстрирован верный ход решения	Продемонстрирован верный ход решения в	Задачи не решены

	системы управления безопасностью информации в автоматизированных системах с учётом знаний проблем и перспектив применения кибернетического оружия в современной сетецентрической войне		получены верные ответы	всех, но не получен верный ответ во всех задачах	большинстве задач	

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) Что такое DDoS-атака?

Ответ:

(1) атака с применением методов социальной инженерии
(2) распределенная атака типа «анализ сетевого трафика»
(3) распределенная атака типа «отказ в обслуживании»
(4) распределенная атака типа «подмена доверенного объекта сети»

2) Какие службы безопасности предназначаются для защиты от атак доступа?

Ответ:

(1) конфиденциальность
(2) целостность
(3) доступность
(4) идентифицируемость

3) Какие службы безопасности предназначаются для защиты от атак модификации?

Ответ:

(1) конфиденциальность
(2) целостность
(3) доступность
(4) идентифицируемость

4) Какое свойство службы безопасности предназначаются для защиты от атак отказа в обслуживании?

Ответ:

(1) конфиденциальность
(2) целостность
(3) доступность
(4) идентифицируемость

5) Какие службы безопасности предназначаются для защиты от атак отказ от обязательств?

   Ответ:

   (1) конфиденциальность
   (2) целостность
   (3) доступность
   (4) идентифицируемость

6) Для защиты от атак какого типа предназначена служба конфиденциальности?

   Ответ:

   (1) атаки доступа
   (2) атаки модификации
   (3) атаки отказа в обслуживании
   (4) атаки отказа от обязательств

7) Для защиты от атак какого типа предназначена служба целостности?

   Ответ:

   (1) атаки доступа
   (2) атаки модификации
   (3) атаки отказа в обслуживании
   (4) атаки отказа от обязательств

8) Для защиты от атак какого типа предназначена служба доступности?

   Ответ:

   (1) атаки доступа
   (2) атаки модификации
   (3) атаки отказа в обслуживании
   (4) атаки отказа от обязательств

9) Для защиты от атак какого типа предназначена служба идентифицируемости?

Ответ:

(1) атаки доступа
(2) атаки модификации
(3) атаки отказа в обслуживании
(4) атаки отказа от обязательств

10) К механизмам физической безопасности относятся:

Ответ:

(1) контроль физической безопасности
(2) правильная настройка компьютерной системы
(3) правильное управление ключами при использовании шифрования

7.2.2 Примерный перечень заданий для решения стандартных задач

1) DoS-атаки чаще всего предпринимаются с использованием

Ответ:

(1) идентификаторов доступа
(2) спецификаторов кодогенерационных последовательностей
(3) фальсификации адреса отправителя
(4) SPAM

2) Модификация сигнатуры без изменения сущности атаки лежит в основе

Ответ:

(1) SPAM
(2) сетевых вирусов
(3) детекторов
(4) каунтеров

3) Методы атак против протокола TCP

Ответ:

(1) атака возможна только в случае, если атакующая машина находится на пути от клиента к серверу
(2) возможна атака за счет сбоя ISN-нумерации пакетов
(3) возможна атака с помощью фальсификации CRC
(4) атаки на TCP-уровне невозможны. Если бы это было не так, стали

бы возможны атаки практически на любые процедуры Интернет, ведь практически все они базируются на протоколе TCP

4) Что такое атака переполнения буфера?

Ответ:

(1) это попытка ввести в HTML-форму больше символов, чем для этого выделено
(2) это попытка переполнить любой программный буфер при вводе символов с клавиатуры
(3) это попытка ввести вместе с текстом какой-то вредоносный код
(4) это попытка передать через сеть более длинное сообщение, чем было запрошено

5) Что происходит при атаках на CGI?

Ответ:

(1) генерация нестандартных строк URL
(2) сбой доступа к серверу DNS
(3) применение метода прямой осцилляции к системным кодам
(4) поражение BIOS

6) В основе атак протокола HTTP лежит

Ответ:

(1) фальсификация методов и заголовков объектов
(2) сбой доступа к стандартным URL
(3) блокировка параметров конфигурации
(4) блокировка доступа к инициализирующим приложениям

7) Что такое "syn flooding"?

Ответ:

(1) метод противодействия DoS-атакам
(2) способ атаковать протокол TCP
(3) вид атаки на ISDN
(4) принцип борьбы с червями

8) Достаточной информацией для атаки DNS извне является

Ответ:

(1) номер используемого UDP-порта
(2) ISN
(3) пароль входа
(4) идентификатор обратной связи

9) Атаки классифицируются и распределяются

Ответ:

(1) по сигнатурам
(2) по времени суток
(3) по сложности распознавания
(4) по методам противодействия

10) Атаки, сопряженные с манипуляциями при обмене сообщениями и фальсификациями заголовков, производятся на протоколы типа

Ответ:

(1) SMTP
(2) IMAP
(3) POP3
(4) NNTP

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Как называется атака, заключающаяся в прослушивании канала связи с использованием специального программно-аппаратного устройства или программы-анализатора пакетов?
Ответ:
(1) анализ сетевого трафика
(2) ложный объект сети
(3) подмена доверенного объекта сети
(4) отказ в обслуживании
2) На каком уровне модели OSI реализуется атака типа «анализ сетевого трафика»?

Ответ:

(1) сетевой
(2) канальный
(3) транспортный
(4) прикладной

3) На каких уровнях модели OSI реализуется атака «Отказ в обслуживании»?

Ответ:

(1) сетевой
(2) канальный
(3) транспортный
(4) прикладной

4) Злоумышленник послал на атакуемый сервер множество SYN-пакетов и не выслал на SYN-ACK пакеты ответы, в результате чего сервер потерял способность устанавливать новые соединения с легальными пользователями. Какая атака была реализована?

Ответ:

(1) анализ сетевого трафика
(2) подмена доверенного объекта сети
(3) отказ в обслуживании
(4) фишинг

5) К какому типу атак относится UDP-flood и ICMP-flood?

Ответ:

(1) анализ сетевого трафика
(2) подмена доверенного объекта сети
(3) отказ в обслуживании
(4) фишинг

6) Как называется атака, при которой злоумышленник генерирует большое количество сообщений с разных источников для почтового сервера, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу?

Ответ:

(1) UDP-flood
(2) ICMP-flood
(3) SYN-flood
(4) Mailbombing

7) Николай получил поддельное письмо от электронной платежной системы с просьбой проверить последние платежи. Ссылка в письме

вела сайт, похожий на официальный сайт платежной системы. Какой атаке подвергся Николай?

Ответ:

(1) анализ сетевого трафика
(2) подмена доверенного объекта сети
(3) отказ в обслуживании
(4) фишинг

8) Какое требование к системе защиты информации предполагает то, что методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления?

Ответ:

(1) адекватность
(2) непрерывность
(3) централизованность
(4) универсальность

9) Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

Ответ:

(1) адекватность
(2) непрерывность
(3) централизованность
(4) универсальность

10) Для чего применяется экранирование помещений и дополнительное заземление объектов защиты?

Ответ:

(1) для увеличения уровня побочных электромагнитных излучений
(2) для уменьшения уровня побочных электромагнитных излучений
(3) для обеспечения бесперебойного питания объектов защиты
(4) для исключения внедрения злоумышленников во внутренние сегменты сети

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

Классификация по характеру воздействия; по цели воздействия; по наличию обратной связи с атакуемым объектом; по условию начала осуществления воздействия; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Примеры.

сбор информации: изучение окружения; идентификация топологии сети; идентификация узлов; идентификация сервисов и сканирование портов; идентификация операционной системы; определение роли узла; определение уязвимостей узла; реализация атаки; проникновение; установление контроля; завершение атаки

фрагментация данных; атака Ping flooding; нестандартные протоколы, инкапсулированные в IP; атака smurf; атака DNS spoofing; атака IP spoofing; навязывание пакетов; Sniffing — прослушивание канала; перехват пакетов на маршрутизаторе; навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки):SYN-flood,UDP-flood

методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети

Популярные фишинговые схемы: несуществующие ссылки; мошенничество с использованием брендов известных корпораций; подложные лотереи; ложные антивирусы и программы для обеспечения безопасности; IVR или телефонный фишинг. Сбор информации из открытых источников: плечевой серфинг; обратная социальная инженерия

Способы защиты от социальной инженерии. Классификация угроз: угрозы, связанные с телефоном; угрозы, связанные с электронной почтой; угрозы, связанные с использованием службы мгновенного обмена сообщениями. Основные защитные методы

Концепция «сетецентрических войн». Наступательные операции в киберпространстве как составная часть информационной войны. Наступательные операции против АСУ инфраструктурных и технологических объектов. Оборонительные операции как часть мер по обеспечению информационной безопасности в мирное время. Перспективы развития концепции кибернетических операций

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент

набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение. Классификация атак	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ
2	Этапы реализации атак	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ
3	Краткое описание некоторых сетевых атак	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ
4	Технологии обнаружения атак	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ
5	Социальная инженерия	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ
6	Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне	ПК-7.3, ПК-7.2	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем

(обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600

Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494

Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101992.html

Дополнительная литература

Белоус, А. И. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия : в 2 книгах / А. И. Белоус, В. А. Солодуха, С. В. Шведов ; под редакцией А. И. Белоуса. — Москва : Техносфера, 2019 — Книга 1 — 2019. — 688 с. — ISBN 978-5-94836-524-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140565

Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163932

Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163812

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://att.nica.ru

http://www.edu.ru/

http://window.edu.ru/window/library

http://www.intuit.ru/catalog/

http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp

https://cchgeu.ru/education/cafedras/kafsib/?docs

http://www.eios.vorstu.ru

http://e.lanbook.com/ (ЭБС Лань)

http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Операции и атаки в информационных системах и сетях» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4