МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Компьютерные преступления в информационно-телекоммуникационных системах и сетях»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ А.Л. Сердечный

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ К.А. Разинкин

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины обеспечить усвоение будущими инженерам, специализирующимся в области организации и технологии защиты информации, поведенческих мотивов, целей, условий и механизмов совершения компьютерных преступлений, а также законодательных основ их предотвращении.

1.2. Задачи освоения дисциплины

✓ привить навыки формирования требований по защите информации в различных КС.

✓ ознакомить с требованиями к защите автоматизированных информационных систем (ИС) от несанкционированного доступа (НСД) на территории Российской Федерации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Компьютерные преступления в информационно-телекоммуникационных 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 «Компьютерные преступления в информационно-телекоммуникационных системах и сетях» направлен на формирование следующих компетенций:

ПК-9.1 - Способен принимать участие в проведении экспертизы при расследовании компьютерных преступлений и исследовании эффективности способов, средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.1	знать виды, технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов знает способы обнаружения и нейтрализации последствий вторжений в компьютерные системы знает методы проведения расследования компьютерных преступлений, правонарушений и инцидентов знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры
	уметь применять нормативные и правовые акты при

	проведении криминалистической экспертизы и криминалистического анализа в процессе расследования компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях; выявлять возможные траектории изменения состояний функционирования компьютерной системы и прогнозировать возможные пути возникновения новых видов компьютерных преступлений
	владеть навыками определения причины и условия изменения свойств исследуемой информации, механизм, динамику и обстоятельства событий по имеющейся информации на носителе данных или ее копиям

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Компьютерные преступления в информационно-телекоммуникационных системах и сетях» составляет 13 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		8	9
Аудиторные занятия (всего)	144	72	72
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	72	36	36
Самостоятельная работа	288	144	144
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	 468 13	 216 6	 252 7

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы компьютерных преступлений	Понятие и разновидность компьютерных преступлений. Характеристика компьютерных преступлений	12	12	48	72
2	Расследование компьютерных преступлений	Обзор угроз политике безопасности компьютерных систем. Перечень моделей Раскрытие и расследование компьютерных преступлений. Законодательная основа борьбы с компьютерными преступлениями	12	12	48	72
3	Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	Детальный анализ вредоносного программного обеспечения. Классификация вирусов. Эвристический анализ. Анализразрушающих воздействий программного обеспечения	12	12	48	72
4	Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	Компьютерные сетевые атаки. Удаленные компьютерные сетевые атаки: распределенные подходы организации. Системы обнаружения вторжения и межсетевого экранирования.	12	12	48	72
5	Противодействие компьютерным преступлениям путём реализации политики безопасности	Анализ разрушающих воздействий. Методы обнаружения и борьбы. Политики безопасности компьютерных систем. Организация сетевой политики безопасности	12	12	48	72
6	Предотвращение компьютерных преступлений в социальной и банковской сферах	Характеристика основных видов преступлений с использованием банковских пластиковых карт. Компьютерные преступления на социальные информационные сети. Предупреждение компьютерных преступлений.	12	12	48	72
		Итого	72	72	288	432

5.2 Перечень лабораторных работ

1. Лабораторная работа № 1. Анализ атаки, ориентированной на взлом программного обеспечения, путём обхода процедуры авторизации.

2. Лабораторная работа № 2. Проведение анализа современного антивирусного программного обеспечения (Avira, Norton AntiVirus, Panda, Kaspersky, McAfee, NOD32, Avast, Dr.Web).

3. Лабораторная работа № 3. Проведения сравнительной характеристики современных межсетевых экранов.

4. Лабораторная работа № 4. Проведение анализа работы сетевых сканеров. (Tcpdump, Sniffer Pro, NetXray, MS Network Monitor, Novell's LanAlyzer, Wireshark).

5. Лабораторная работа № 5. Проведение анализа системы обнаружения вторжений Snort.

6. Лабораторная работа № 6. Проведение анализа подсистемы безопасности в семействе ОС Windows.

7. Лабораторная работа № 7. Проведение анализа подсистемы

безопасности в ОС Unix.

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Расследование компьютерных преступлений в РКС, осуществляемых с использованием web-технологий».

Задачи, решаемые при выполнении курсового проекта:

- закрепить знание основных принципов построения защищённых РКС;
- закрепить знания особенностей защиты информации на узлах компьютерной сети, основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

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-9.1	знать виды, технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов знает способы обнаружения и нейтрализации последствий вторжений в компьютерные системы знает методы проведения расследования компьютерных преступлений, правонарушений и инцидентов	знание видов, технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов знает способы обнаружения и нейтрализации последствий вторжений в компьютерные системы знает методы проведения расследования компьютерных преступлений, правонарушений и инцидентов знает руководящие и методические документы уполномоченных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры	федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры		
	уметь применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа в процессе расследования компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях; выявлять возможные траектории изменения состояний функционирования компьютерной системы и прогнозировать возможные пути возникновения новых видов компьютерных преступлений	умение применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа в процессе расследования компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях; выявлять возможные траектории изменения состояний функционирования компьютерной системы и прогнозировать возможные пути возникновения новых видов компьютерных преступлений	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками определения причины и условия изменения свойств исследуемой информации, механизм, динамику и обстоятельства событий по имеющейся информации на носителе данных или ее копиям	владение навыками определения причины и условия изменения свойств исследуемой информации, механизм, динамику и обстоятельства событий по имеющейся информации на носителе данных или ее копиям	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8, 9 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-9.1	знать виды, технологии поиска и анализа следов	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных

	компьютерных преступлений, правонарушений и инцидентов знает способы обнаружения и нейтрализации последствий вторжений в компьютерные системы знает методы проведения расследования компьютерных преступлений, правонарушений и инцидентов знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры					ответов
	уметь применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа в процессе расследования компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях; выявлять возможные траектории изменения состояний функционирования компьютерной системы и прогнозировать возможные пути возникновения 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
	владеть навыками определения причины и условия изменения свойств исследуемой информации,	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные	Продемонстрирован верный ход решения всех, но не получен верный ответ	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	механизм, динамику и обстоятельства событий по имеющейся информации на носителе данных или ее копиям		ответы	во всех задачах		

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. Какие преступления относятся к преступлениям в сфере компьютерной информации?

а) создание вредоносных компьютерных программ;

б) распространение порнографических материалов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

г) все ответы правильные.

2. Родовым объектом преступлений в сфере компьютерной информации являются:

а) экономическая безопасность;

б) отношения в сфере охраны авторского права;

в) информационная безопасность;

г) общественная безопасность и общественный порядок.

3. Субъектом преступлений в сфере компьютерной информации является:

а) юридическое или физическое лицо, не имеющие разрешения для работы с информацией определенной категории;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) физическое, вменяемое лицо, достигшее 16-летнего возраста;

г) физическое лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

4. К компьютерной информации относятся:

а) собственно информационные ресурсы (базы данных, текстовые, графические файлы и т.д.), представленные в форме электрических сигналов;

б) программы, обеспечивающие функционирование компьютера или информационно-телекоммуникационных сетей, хранение, обработку и передачу данных;

в) информация на машинном носителе, в компьютере или информационно-телекоммуникационных сетях;

г) все ответы правильные.

5. Преступление, предусмотренное ст. 272 УК РФ «Неправомерный

доступ к компьютерной информации» считается оконченным:

а) с момента совершения неправомерного доступа к охраняемой законом компьютерной информации;

б) только в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) только при наступлении тяжких последствий в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

г) все ответы правильные.

6. В ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» не предусмотрена уголовная ответственность за:

а) внесение изменений в существующие программы;

б) распространение машинных носителей с вредоносными программами;

в) несанкционированное копирование охраняемой законом компьютерной информации;

г) нет правильного ответа.

7. Преступление, предусмотренное ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», считается оконченным:

а) только при наступлении тяжких последствий;

б) только в случае несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) с момента использования или распространения вредоносной программы;

г) с момента создания, использования или распространения вредоносной программы.

8. Субъектом преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», является:

а) физическое, вменяемое лицо, достигшее 16-летнего возраста;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) лицо, имеющее право на доступ к компьютеру или информационно-телекоммуникационным сетям;

г) лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

9. В числе квалифицирующих признаков в ст. 273 УК РФ предусмотрено совершение данного преступления:

а) с целью скрыть другое преступление или облегчить его совершение;

б) из корыстной заинтересованности;

в) из хулиганских побуждений;

г) по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

10. Преступление, предусмотренное ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», считается оконченным:

а) с момента нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

б) с момента уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) если это деяние причинило крупный ущерб;

г) только при наступлении тяжких последствий.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

LWM+

На основе анализа угроз

С полным перекрытием

Лендвера

2. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется

мандатным+

привилегированным

идентифицируемым

избирательным

3. На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс

C1+

B2

C2

B1

4. Наименее затратный криптоанализ для криптоалгоритма DES

перебор по всему ключевому пространству+

разложение числа на сложные множители

разложение числа на простые множители

перебор по выборочному ключевому пространству

5. Наукой, изучающей математические методы защиты информации путем ее преобразования, является

криптология+

криптоанализ

стеганография

криптография

6. Недостатком модели конечных состояний политики безопасности является

сложность реализации+
изменение линий связи
статичность
низкая степень надежности

7. Недостаток систем шифрования с открытым ключом

относительно низкая производительность+
необходимость распространения секретных ключей
при использовании простой замены легко произвести подмену одного шифрованного текста другим
на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

8. Основу политики безопасности составляет

способ управления доступом +
программное обеспечение
управление риском
выбор каналов связи

9. По документам ГТК количество классов защищенности АС от НСД

9 +
6
8
7

10. По документам ГТК самый высокий класс защищенности СВТ от НСД к информации

1 +
9
7
6

11. Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа

компрометация
уборка мусора
наблюдение
перехват

12. При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается

тип разрешенного доступа +
объект системы
субъект системы
факт доступа

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Какие системы предназначены для обеспечения сетевого мониторинга, анализа и оповещения в случае обнаружения сетевой атаки?

IDP +

AV

WCF

IPS

2. Какие системы предназначены для обеспечения сетевого мониторинга, анализа, оповещения в случае обнаружения сетевой атаки, а также способны ее блокировать?

IDP

AV

WCF

IPS +

3. В чем заключается отличие вторжений от вирусных атак?

вторжения обычно содержатся в отдельном загрузочном файле, который закачивается в систему пользователя

вторжения по характеру воздействия на атакуемую сеть могут быть как негативные, так и нейтральные

+ вторжения проявляются как образцы вируса, нацеленные на поиск путей преодоления механизмов обеспечения безопасности

вторжения могут осуществляться посредством сети

4. Как система IDP в NetDefend обнаруживает вторжения?

по сигнатурам вирусов и атак +

по адресу отправителя трафика

на основе статистического анализа

с помощью поля ESP в составе передаваемых данных

5. В 2016 году были украдены данные 412 миллионов аккаунтов сайта для «взрослых» знакомств AdultFriendFinder (AFF). Злоумышленники воспользовались LFI — local file inclusion — на одном из серверов. А что это такое?

Возможность изменения и выполнения локальных файлов на серверной стороне.+

Уязвимость в процессе копирования при записи, из-за которой пользователь мог повысить свои привилегии.

Аппаратная ошибка процессора, позволяющая получить доступ к виртуальной памяти сервера.

6. Вишенкой на торте взлома AdultFriendFinder оказалась не только БД с личными данными пользователей, но и сами пароли, которые было не так сложно восстановить из хэша. А какой алгоритм использовался для их хеширования?

SHA-3

SHA-2

SHA-1+

MD5

7. В 2017 году одной из самых чувствительных утечек стал взлом кредитного бюро Equifax. Тогда были украдены личные и финансовые данные 149 миллионов американцев: дата рождения, адреса проживания, номера страховок и водительских удостоверений. Взлом Equifax имеет не только экономические последствия: в совокупности с данными из других источников он представляет собой материал для анализа с помощью AI или ML и может быть использован в шпионских целях. К утечке привела уязвимая версия Apache Struts на одном из серверов. Как думаете, сколько времени ее не обновляли?

Неделя

Месяц

2,5 месяца

4,5 месяцев +

8. В этом году было несколько примеров атак на цепь поставок (Supply chain attack), когда злоумышленники действовали не напрямую, а через доверенных партнёров. Свежий пример — атака на индийского аутсорс-гиганта Wipro, чьи сотрудники имеют доступ во внутренние сети европейских и американских компаний. Через Wipro преступники внедрились к его клиентам и установили на компьютерах программу

для удалённого доступа. А вы догадаетесь, какую именно?

TeamViewer

Ammyy Admin

ScreenConnect+

RDP

9.Еще одной головной болью специалистов по безопасности являются облачные сервисы. В 2017 году в облачном хранилище Amazon была обнаружена открытая база данных 200 млн американских избирателей. Информация была бережно подготовлена и систематизирована для аналитической работы и принадлежала компании Deep Root Analitics, которая обрабатывала их по заказу Республиканской партии. Для доступа к ней было достаточно...

Знать URL или перейти на внутренний субдомен dra-dw (Deep Root Analytics Data Warehouse)+

Использовать стандартную связку логин/пароль: administrator/qwerty

Быть клиентом Deep Root Analytics и зайти под своей учетной записью.

Скачать по ссылке с официального сайта Deep Root Analytics в разделе техническая поддержка

10.Даже небольшая ошибка с правами доступа может привести к неприятным последствиям. В этом году с этим столкнулась Почтовая служба США. Любой желающий мог получить доступ к данным 60 млн пользователей и информации о движении коммерческих грузов. Для этого было достаточно:

Использовать SQL-инъекции на сайте при поиске почтового отправления.

Знать URL или внутренний субдомен dra-dw облачного сервера Почтовой службы

Используя свои учетные данные, подключиться к сервисам USPS по API.+

11. Человеческий фактор до сих пор остается одним из самых слабых мест в информационной безопасности. В 2016 году в этом убедился Uber, у которого украли данные 57 млн водителей и клиентов. Компания потеряла 200 млн долларов на компенсациях и получила огромный удар по репутации, когда появилась информация, что она заплатила злоумышленникам 100 000$ и целый год скрывала факт взлома. Догадайтесь, как хакеры получили доступ к учетным данным сотрудникам Uber?

Злоумышленникам продала данные уборщица, которая заметила пароли на стикерах возле мониторов.

Один из системных администраторов Uber выложил на одном из форумов файл конфигурации сетевого коммутатора Cisco со своими учётными данными для входа во внутреннюю сеть.

У одного из разработчиков украли смартфон, где хранились данные для входа во внутреннюю сеть Uber.

Два разработчика выложили логин и пароль для входа во внутреннюю сеть Uber в коде на GitHub.+

12. Киберугрозы могут быть направлены не только на информацию, но и на физическую инфраструктуру. До выжигания мозга, как у Гибсона, пока не дошли, но вот перепрограммировать работу ПЛК (программируемые логические контроллеры) вредоносное ПО сможет. А кто умел это делать:

WannaCry
Stuxnet+
Bad Rabbit
Regin

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

1. Понятие «компьютерные преступления». Два основных подхода.
2. Криминалистическое толкование компьютерных преступлений.
3. Состав компьютерных преступлений.
4. Классификация компьютерных преступлений в Российской Федерации.
5. Законодательная база в области компьютерных преступлений России. Ответственность за совершение компьютерных преступлений различного характера.

6. Международный кодификатор компьютерных преступлений.
7. Незаконные воздействия на компьютерную информацию.
8. Система обеспечения оперативно-розыскных мероприятий.
9. Зарубежное законодательство в области компьютерных преступлений.
10. Политика безопасности. Жизненный цикл компьютерной системы. Угрозы компьютерной системе.
11. Канал утечки. Виды каналов утечки.
12. Описание моделей безопасности с использованием субъектов и объектов.
13. Дискретные модели безопасности.
14. Модель Адепт.
15. Пространство Хартстона.
16. Матрица доступа.
17. Модель Харрисона, Руззо и Ульмана.
18. Модель Take Grant.
19. Модель управления доступом.
20. Модели на основе анализа угроз системе.
21. Игровая модель.
22. Модель системы безопасности с полным перекрытием.
23. Модели конечных состояний.
24. Модель уровней секретности.
25. Модель Белла-Лападула.
26. Модель китайской стены.
27. Модель Low-Water-Mark (Биба).
28. Модель Лендвера.
29. Модель Кларка-Вилсона.
30. Модель Липнера.
31. Признаки, по которым можно классифицировать вирусы.
32. Классификация вирусов по среде обитания.
33. Классы вредоносного программного обеспечения.
34. Загрузочные вирусы. Принцип работы.
35. Технологии встраивания вируса в MBR и BR.
36. Файловые вирусы.
37. Перезаписывающие, паразитические, вирусы без точки входа.
38. Компаньон-вирусы, файловые черви, Link-вирусы.
39. OBJ-, LIB-вирусы и вирусы в исходных текстах.
40. Вирусы семейства Macro. Характерные примеры проявлениями вирусов семейства macro.
41. Полиморфик вирусы. Уровни полиморфизма.
42. Стелс-вирусы: загрузочные, файловые, макро.
43. Резидентные вирусы. Характеристики резидентных вирусов.
44. Утилиты скрытого администрирования.
45. Троянский конь. Логическая бомба.
46. Полиморфные генераторы. Сетевые вирусы.

47. Методы обнаружения и удаления компьютерных вирусов.
48. Типы антивирусов.
49. Сканеры, CRC-сканеры, Блокировщики, Иммунизаторы.
50. Ложное срабатывание. Сканирование по запросу. Сканирование на лету.
51. Обнаружение неизвестного вируса. Проникновение в таблицу векторов прерываний. Встраивание в DOS. Другие способы проникновения.
52. Обнаружение загрузочного вируса.
53. Обнаружение макро-вируса.
54. Профилактика вирусного заражения компьютера. Основные правила защиты.
55. Восстановление пораженных вирусами объектов.
56. Уязвимость. Угроза. Атака. Компоненты сетевой атаки.
57. Классификация сетевых атак по составу.
58. Модели традиционных атак.
59. Классификация сетевых атак по применению. Коммутируемая инфраструктура. Анти-снифферы.
60. IP-spoofing. Противодействие спуфингу. Отказ в обслуживании. Противодействие.
61. Атаки типа Main-in-the-Middle.
62. Атаки на уровне приложений. Противодействие.
63. Сетевая разведка. Злоупотребление доверием.
64. Переадресация портов при сетевом взаимодействии.
65. Уровни модели ISO/OSI.
66. Классификация удаленных атак на распределенные вычислительные системы.
67. Анализ сетевого трафика.
68. Способы атаки типа анализ сетевого трафика.
69. Подмена доверенного объекта или субъекта распределенной сети.
70. Внедрение в распределенную сеть ложного объекта путем навязывания ложного маршрута.
71. Атака типа «Ложный ARP-сервер». Сценарий реализации.
72. Реализация атаки типа ложный DNS-сервер. Сценарий 1: злоумышленник в одном сегменте сети с DNS-сервером, но в разных сегментах с атакуемым объектом. Сценарий 2: злоумышленник в одном сегменте сети с атакуемым хостом, но в разных сегментах с DNS-сервером. Шторм DNS-запросов.
73. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания ложного маршрутизатора.
74. Принцип подмены одного из субъектов TCP-соединения в сети Internet.
75. IDS-системы.
76. Три основных подхода к обнаружению атак с помощью IDS-систем.
77. Недостатки современных систем обнаружения.

78. Хостовая и сетевая IDS. Характеристики.

79. Атаки на IDS (Fragmentation Reassembly Timeoutattacks, TTL Basedattacks, OverlappingFragments).

80. Сигнатурные и поведенческие IDS.

81. Распределённые системы обнаружения вторжений.

82. Системы предотвращения вторжений.

83. Определение новых методов сетевых вторжений.

84. Варианты реакций на обнаруженную атаку с помощью IDS.

85. Выявление злоупотреблений при анализе сетевых атак. Эвристический анализ.

86. Состав и структура аппаратной реализации системы обнаружения вторжений.

87. Преступления, совершаемые с использованием банковских карт.

88. Классификация банковских карт.

89. Уязвимости механизма функционирования банковских карт в привязке к процессинговому центру, банкам эмитента и эквайрера.

90. Анализ состояний информационной безопасности в работе процессингового центра.

91. Личность компьютерного преступника.

92. Два подхода к определению личности преступника.

93. Раскрытие и расследование компьютерных преступлений.

Типовые следственные ситуации первоначального этапа и следственные действия в области раскрытия компьютерных преступлений.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

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	Основы компьютерных преступлений	ПК-9.1	Тест, защита лабораторных работ, сдача курсовых работ
2	Расследование компьютерных	ПК-9.1	Тест, защита

	преступлений		лабораторных работ, сдача курсовых работ
3	Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	ПК-9.1	Тест, защита лабораторных работ, сдача курсовых работ
4	Противодействие компьютерным преступлениям, реализуемым входе проведения компьютерных сетевых атак	ПК-9.1	Тест, защита лабораторных работ, сдача курсовых работ
5	Противодействие компьютерным преступлениям путём реализации политики безопасности	ПК-9.1	Тест, защита лабораторных работ, сдача курсовых работ
6	Предотвращение компьютерных преступленийв социальной и банковской сферах	ПК-9.1	Тест, защита лабораторных работ, сдача курсовых 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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Эпидемии в телекоммуникационных сетях [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN

978-5-9912-0682-2 : 736-00.

2. Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 247 с. : ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6 : 708-00.

3. Социальные сети и деструктивный контент [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 274 с. : ил. - (Теория сетевых войн. № 3). - Библиогр.: с. 224-239 (278 назв.). - ISBN 978-5-9912-0686-0 : 719-00.

4. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем: Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

5. Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература:

1. Обнаружение сетевых вторжений [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (423 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2. Модели обнаружения сетевых вторжений [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (652 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

3. Методические указания к курсовому проектированию по дисциплине «Компьютерные преступления в распределенных компьютерных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Г. А. Остапенко, А. Е. Дешина. - Электрон. текстовые, граф. дан. (820 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

4. Методические указания к самостоятельным работам по дисциплине «Компьютерные преступления в распределенных компьютерных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Г. А. Остапенко, А. Е. Дешина. - Электрон. текстовые, граф. дан. (427 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

5. Остапенко, Г.А. Логико-лингвистические модели атак на компьютерные системы [Электронный ресурс] : Учеб. пособие / под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (8452435 байт). - Воронеж :

ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

6. Компьютерные преступления в сфере государственного и муниципального управления / В. Г. Кулаков, А. К. Соловьев, В. Г. Кобяшов; под. ред. А. Г. Остапенко. - Воронеж: ВИ МВД России, 2002. - 116 с. - ISBN 5-88591-002-4: 20.00.

7. Остапенко, Г.А. Компьютерные преступления [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,37 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

8. Дуров В.П. Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :6681088 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

9. Моделирование информационных операций и атак в сфере государственного и муниципального управления: Монография / под ред. В.И. Борисова. - Воронеж: ВИ МВД России, 2004. - 144 с. - 100-00.

10. Оптимальный синтез и анализ эффективности комплексов защиты информации: Монография / В. Г. Кулаков [и др.]. - Воронеж: ВГТУ, 2006. - 137 с. - 30-00

11. Остапенко, Г.А. Нейронные модели обнаружения вторжений и атак на компьютерные сети [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 2402Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

12. Щербаков, В.Б. Обнаружение вторжений на основе анализа фрагментов унитарного кода [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 1454 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

13. Пархоменко, А.П. Основные проблемы и особенности защиты информации в банковских системах: модели нарушителей [Электронный ресурс] / под ред. Г. С. Остапенко. - Электрон. текстовые, граф. дан. (1245435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00

14.Компьютерные преступления [Электронный ресурс] : Методические указания к выполнению практических занятий по учебной дисциплине "Компьютерные преступления в распределительных компьютерных системах" для студентов специальности 090301 "Компьютерная безопасность" очной формы обучения / Каф. систем информационной безопасности; Сост.: Г. А. Остапенко, К. В. Симонов. - Электрон. текстовые, граф. дан. (3478 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 00-00.

15. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

16. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология.

Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности

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:

1. http://www.edu.ru – портал Министерства образования и науки РФ
2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям
   http://www.consultant.ru/document/cons_doc_LAW_220885/
6. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
7. Трудовой кодекс РФ. Глава 14. https://www.msu.ru/info/is/docs/1/197fz.pdf
8. Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_389271/
9. Сайт Банка данных угроз безопасности информации ФСТЭК России. https://fstec.ru/
10. Операционная система Kali Linux, содержащая средства демонстрации компьютерных атак, а также средства контроля защищённости информационных систем методом тестирования на проникновение https://www.kali.org/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

1. Комплект действующих нормативных документов в области компьютерных преступлений и обеспечения безопасности информационных систем.
2. Компьютерный класс и компьютерные программы для демонстрации компьютерных сетевых атак и мер защиты от них.

Проектор и ноутбук.

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

По дисциплине «Компьютерные преступления в информационно-телекоммуникационных системах и сетях» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

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.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

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 зачетом с оценкой, 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