МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического моделирования


М.Ш. Бурлуцкая

02.07.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.07 Тактики и техники реализации компьютерных атак

1. Код и наименование специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра математического моделирования

6. Составители программы: Куликов С.С., к.ф.-м.н., доцент кафедры математического моделирования

7. Рекомендована: Научно-методическим советом математического факультета, протокол № 0500-07 от 29.06.2021

8. Учебный год: 2023/2024 **Семестр(ы):** 6

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

- изучение подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности систем и их информационной инфраструктуры;
- изучение аспектов компьютерной безопасности, начиная от стратегии защиты до управления уязвимостями, изучение различных отраслевых стандартов и методов реагирования, процессов взлома данных и политики безопасности, базовых средств контроля безопасности.

Задачи учебной дисциплины:

- научиться формализовать задачу управления безопасностью информационных систем и моделировать угрозы безопасности информации;
- дать представление о методах атак и шаблонов, позволяющих распознавать аномальное поведение в организации, с помощью тактических приемов;
- ознакомление с различными отраслевыми стандартами и передовыми методами реагирования..

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Тактики и техники реализации компьютерных атак» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули).

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен обеспечивать функционирование средств защиты информации в информационно-аналитических системах	ПК-1.2	Способен администрировать системы защиты информации от несанкционированного доступа и воздействия	Знать: способы обнаружения и нейтрализации последствий вторжений в компьютерные системы Уметь: анализировать защищенность систем, администрировать системы обнаружения компьютерных атак Владеть: навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак
		ПК-1.3	Способен администрировать системы обнаружения и предотвращения компьютерных атак	
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.2	Способен моделировать угрозы безопасности информации	Знать: основные принципы построения защищенных распределенных компьютерных систем Уметь: формализовать задачу управления безопасностью информационных систем Владеть: навыками выявления и устранения уязвимостей компьютерной сети

12. Объем дисциплины в зачетных единицах/час. — 2/72.

Форма промежуточной аттестации: зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			6 семестр	
Контактная работа		48	48	
в том числе:	лекции	32	32	
	практические	0	0	
	лабораторные	16	16	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		24	24	
Промежуточная аттестация				
Итого:		**72**	**72**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Системный подход к обеспечению защиты от компьютерных атак	1. Компьютерные системы и их компоненты как объекты защиты. 2. Угрозы безопасности и каналы их воздействия. 3. Направления и методы защиты информации 4. Методика построения защищенных компьютерных систем. 5. Организационные методы и средства защиты компьютерных систем.	
1.2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	6. Системы обнаружения атак (Intrusion Detection Systems, IDS)	
	Практика применения	7. Методы и средства оценки защищенности компьютерных систем. 8. Средства моделирования атак и воздействия различных угроз на компоненты КС 9. Средства контроля доступа к компонентам компьютерных систем. 10. Методы и средства обеспечения безопасности электропитания компьютерных систем 11. Методы и средства гарантированного уничтожения информации. 12. Методы и средства выявления и локализации утечек информации по техническим каналам. 13.	
2. Практические занятия			

3. Лабораторные занятия			
3.1	Системный подход к обеспечению защиты от компьютерных атак	1. Примеры современных КС. Характеристика компонентов КС с точки зрения уязвимости к воздействию угроз безопасности. 2. Характеристика системы ЗИ для сложных КС. Методика построения комплексных систем защиты КС. 3. Установление режимов доступа к информации, циркулирующей в КС. Администрирование КС	
3.2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	4. Системы обнаружения атак (Intrusion Detection Systems, IDS).	
	Практика применения	5. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков. 6. Характеристика носителей и стандартных способов записи/удаления информации. Описание технических средств гарантированного удаления информации. 7. Инженерные СЗИ от ПЭМИН. Классификация и характеристика пассивных и активных СЗИ от ПЭМИН	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Системный подход к обеспечению защиты от компьютерных атак	12		6	10	28
2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	4		2	4	10
3	Практика применения	16		8	10	34
	Итого:	32		16	24	72

14. Методические указания для обучающихся по освоению дисциплины:

Изучение дисциплины требует систематического и последовательного накопления знаний. Студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на лабораторных занятиях. Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций и лабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность, на которую отводится 24 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Тактики и техники реализации компьютерных атак» предполагает выполнение следующих заданий:

1) самостоятельное изучение учебных материалов по разделам дисциплины с использованием основной и дополнительной литературы, информационно-справочных и поисковых систем;

2) подготовку к текущим аттестациям: выполнение лабораторных заданий по поиску необходимых для работы в аудитории материалов в Интернете.

Все выполняемые студентами самостоятельно задания подлежат последующей проверке преподавателем для получения допуска к зачету.

В случае необходимости перехода на дистанционный режим обучения будет создан электронный курс «Название» на портале «Электронный университет ВГУ»: edu.vsu.ru. Там же будут размещены необходимые для усвоения курса материалы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Милославская Н. Г. - Сетевые атаки на открытые системы на примере интранета - Москва: МИФИ, 2012. http://biblioclub.ru/inde 1x.php?page=book&id=231630
2	Мэйволд, Э. Безопасность сетей : учебное пособие : [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035

б) дополнительная литература:

№ п/п	Источник
3	Сергеева, Ю. С. Защита информации: конспект лекций : учебное пособие : [16+] / Ю. С. Сергеева. – Москва : А-Приор, 2011. – 128 с. – (Конспект лекций. В помощь студенту). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=72670
4	Докучаев В.А., Кондратьев М.Г., Крупнов И.А., Маклачкова В.В., Мытенков С.С., Шведов А.В., Докучаев В.А. - Система обнаружения компьютерных атак «Форпост»: учебно-методическое пособие - Москва: Московский технический университет связи и информатики, 2016.
5	Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
6	Электронный каталог ЗНБ ВГУ : http://www.lib.vsu.ru .
7	https://math.vsu.ru/wp/?page_id=937 – раздел на сайте математического факультета, на котором размещены методические издания.
8	ЭБС «Университетская библиотека онлайн».
9	Электронный университет ВГУ : https://edu.vsu.ru/ .

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики .— Москва : Издательский дом Высшей школы экономики, 2015 .— 574 с. URL:http://biblioclub.ru/index.php?page=book&id=440285>.
2	Сергеева, Ю. С. Защита информации: конспект лекций : учебное пособие : [16+] / Ю. С. Сергеева. – Москва : А-Приор, 2011. – 128 с. – (Конспект лекций. В помощь студенту). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=72670
3	Докучаев В.А., Кондратьев М.Г., Крупнов И.А., Маклачкова В.В., Мытенков С.С., Шведов А.В., Докучаев В.А. - Система обнаружения компьютерных атак «Форпост»: учебно-методическое пособие - Москва: Московский технический университет связи и информатики, 2016.
4	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ» (https://edu.vsu.ru).

Перечень необходимого программного обеспечения: Win10pro или Linux, Microsoft Office, LibreOffice 6, Calc, Microsoft Visual Studio, Microsoft Visual C++, Foxit Reader, браузер Mozilla Firefox, Opera или Internet. Wireshark (Свободное программное обеспечение GNU GPL 2), Snort (Свободная лицензия GNU GPL)

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации со специализированной мебелью.

Для лабораторных работ и самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Системный подход к обеспечению защиты от компьютерных атак	ПК-1 ПК-2	ПК-1.2 ПК-1.3 ПК-2.2	Устный опрос Реферат Лабораторная работа
2.	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.			
3.	Практика применения			
Промежуточная аттестация Форма контроля – зачет				Перечень вопросов к зачету

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: устных опросов, проверки домашних заданий, лабораторных работ, , защиты рефератов.

Перечень лабораторных работ:

1. Оценка агентов угроз и угроз Разработка классификации агентов угроз Упорядочивание угроз и механизмов угроз в соответствии с классификацией

агентов угроз Оценка вероятности угроз, инициируемых преднамеренными агентами Оценка уязвимости

2. Оценка политик безопасности
3. Создание модели политики безопасности индивидуального предприятия на основе собранных данных

Темы для рефератов:

1. Процесс реагирования на компьютерные инциденты
2. Жизненный цикл атаки
3. Разведка и сбор данных
4. Охота на пользовательские реквизиты
5. Проверка политики безопасности
6. Системы обнаружения вторжений
7. Инструментальные средства кибербразведки с открытым исходным кодом
8. Исследование скомпрометированной системы внутри организации
9. Создание стратегии управления уязвимостями
10. Передовые методы управления уязвимостями
11. Журналы операционной системы

Для оценивания текущего контроля успеваемости используются следующие ***показатели:***

1. знание основных понятий и методов;
2. умение применять полученные знания и навыки для решения проблем, проводить анализ полученных решений;
3. умение писать код компьютерных программ для решения типовых задач;
4. знание имеющихся ресурсов для решения прикладных задач;
5. умение использовать стандартные пакеты программного обеспечения для решения типовых задач;
6. владение навыками хранения, поиска, сбора, систематизации, обработки и использования информации.

Шкала оценок:

Зачтено: Выполнение заданий соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.

Не зачтено: Ответы не соответствуют ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.

20.2. Промежуточная аттестация

Допуском к промежуточной аттестации является выполнение лабораторных работ и защита реферата.

Промежуточная аттестация по дисциплине осуществляется в форме собеседования по вопросам с помощью нижеприведенных оценочных средств (перечень вопросов к зачету).

Перечень вопросов к зачету:

1. Компьютерные системы и их компоненты как объекты защиты.
2. Угрозы безопасности и каналы их воздействия.
3. Направления и методы защиты информации
4. Методика построения защищенных компьютерных систем.
5. Организационные методы и средства защиты компьютерных систем.
6. Системы обнаружения атак (Intrusion Detection Systems, IDS)
7. Методы и средства оценки защищенности компьютерных систем.
8. Средства моделирования атак и воздействия различных угроз на компоненты КС
9. Средства контроля доступа к компонентам компьютерных систем.
10. Методы и средства обеспечения безопасности электропитания компьютерных систем
11. Методы и средства гарантированного уничтожения информации.
12. Методы и средства выявления и локализации утечек информации по техническим каналам.

Для оценивания результатов обучения на зачете используются следующие **показатели:**

1) знание теоретических основ;
2) успешное прохождение текущей аттестации.

Для оценивания результатов используется шкала: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания	Шкала оценок
Ответ соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные.	«Зачтено»
Ответ не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.	«Не зачтено»