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

УТВЕРЖДАЮ
Заведующий кафедрой
математического моделирования


М.Ш. Бурлуцкая

16.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.02 Тактики и техники реализации компьютерных атак

1. Код и наименование специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Информационная безопасность финансовых и экономических структур

3. Квалификация выпускника:Специалист по защите информации

4. Форма обучения:Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра математического моделирования

6. Составитель программы:Куликов Сергей Сергеевич, к.т.н., доцент

7. Рекомендована:Научно-методическим советом математического факультета,протокол № 0500-03 от 28.03.2024

8. Учебный год: 2026/2027 **Семестр:**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 ихинформационной инфраструктуры;
- изучение аспектов компьютерной безопасности, начиная от стратегии защитыдо управления уязвимостями, изучение различных отраслевых стандартов и методовреагирования, процессов взлома данных и политики безопасности, базовых средствконтроля безопасности.

Задачи учебной дисциплины:

- научиться формализовать задачу управления безопасностьюинформационных систем и моделировать угрозы безопасности информации;
- дать представление о методах атак и шаблонов, позволяющих распознаватьаномальное поведение в организации, с помощью тактических приемов;
- ознакомление с различными отраслевыми стандартами и передовымиметодами 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: основные средства защиты информации в ИАС; Уметь: администрировать системы защиты информации от несанкционированного доступа и воздействия; Владеть: навыкамиадминистрирования систем обнаружения и предотвращения 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: способы и методы анализа безопасности информации с помощью формальных моделей; Уметь: моделировать угрозы безопасности информации; Владеть: навыкамианализа защищенности информационных систем.

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	1. Системыобнаруженияатак (Intrusion Detection Systems, IDS).	
1.3	Практика применения	1. Методы и средства оценки защищенности компьютерных систем. 2. Средства моделирования атак и воздействия различных угроз на компоненты КС. 3. Средства контроля доступа к компонентам компьютерных систем. 4. Методы и средства обеспечения безопасности электропитания компьютерных систем. 5. Методы и средства гарантированного уничтожения информации. 6. Методы и средства выявления и локализации. утечек информации по техническим каналам.	
2. Лабораторные занятия			
2.1	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.	
2.2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности	1. Системыобнаруженияатак (Intrusion Detection Systems, IDS).	
2.3	Практика применения	1. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков. 2. Характеристика носителей и стандартных способов записи/удаления информации. Описание технических средств гарантированного удаления информации. 3. 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. Студентамрекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затрудненияхвосприятии материала следует обращаться к основным литературным источникам, к лектору (по графику егоконсультаций) или к преподавателю на лабораторных занятиях. Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций илабораторных 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.

Вопросы лекционных и лабораторных занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную

позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольных и лабораторных работ) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации.

В случае необходимости перехода на дистанционный режим обучения будет создан электронный курс «Тактики и техники реализации компьютерных атак»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 / Н.Г. Милославская. - 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.	Диогенес Ю. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, Э. Озкайя : пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.
4.	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 .
5.	Система обнаружения компьютерных атак / В.А. Докучаев, М.Г. Кондратьев, И.А. Крупнов, В.В. Маклачкова, С.С.Мытенков, А.В. Шведов. - «Форпост»: учебно-методическое пособие - Москва: Московский техническийуниверситет связи и информатики, 2016.

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

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

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1.	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 .
2.	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>.
3.	Система обнаружения компьютерных атак / В.А. Докучаев, М.Г. Кондратьев, И.А. Крупнов, В.В. Маклачкова, С.С.Мытенков, А.В. Шведов. - «Форпост»: учебно-методическое пособие - Москва: Московский техническийуниверситет 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 MozillaFirefox, 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 и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебельКомпьютерный класс: специализированная мебель, маркерная доска, персональные компьютеры.

Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop)

Visual Studio Community (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/)

LibreOffice (GNU Lesser General Public License (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/).

В самостоятельной работе обучающиеся используют ресурсы Зональной научной библиотеки ВГУ(электронный каталог: http://www.lib.vsu.ru).

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	Оценочныесредства
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 киберразведки 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. Системыобнаруженияатак (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»

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

Перечень заданий для оценки сформированности компетенции:

№	Вопрос	Варианты ответов	Правильный ответ
1	Сетевой атакой, цель которой заключается в выявлении работающих в сети служб, открытых портов, активных сетевых сервисов, используемых протоколов, является:	А) Анализ сетевого трафика. Б) Сканирование сети. В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	А) Анализ сетевого трафика.
2	Сетевой атакой, цель которой заключается в создании таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён, является:	А) Анализ сетевого трафика. Б) Сканирование сети. В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	Г) Атака «отказ в обслуживании».
3	Сетевой атакой, в результате реализации которой нарушитель	А) Атака «Человек по-середине». Б) Сканирование сети.	А) Атака «Человек по-

	получает возможность перехватывать и передавать в канал связи сетевой трафик, является:	В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	середине».
4	Атаки, нарушающие работу протоколов маршрутизации, реализуются на:	А) Физическом уровне. Б) Канальном уровне. В) Сетевом уровне. Г) Прикладном уровне.	Г) Прикладном уровне.
5	Атака переполнения таблицы коммутации реализуется на:	А) Физическом уровне. Б) Канальном уровне. В) Сетевом уровне. Г) Прикладном уровне.	Б) Канальном уровне.
6	Сканирование портов осуществляется на:	А) Канальном уровне. Б) Сетевом уровне. В) Транспортном уровне. Г) Прикладном уровне.	В) Транспортном уровне.
7	Для восстановления прообраза по известному хеш-значению не может использоваться:	А) Брутфорс-атака. Б) Радужные таблицы. В) Обратное преобразование. Г) Перебор по словарю.	В) Обратное преобразование.
8	Аббревиатура APT означает:	-	Целевая атака
9	Вид интернет-мошенничества и компьютерных атак, цель которых получить идентификационные данные пользователей или иную конфиденциальную информацию за счет создания ложных интерфейсов, писем и иных доверенных объектов, называется:	-	Фишинг
10	База данных (матрица), содержащая информацию о тактиках и техниках компьютерных атак, называется:	-	MITRE ATT&CK

Критерии и шкалы оценивания заданий ФОС:

I. Тестовые задания.

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- за каждый верный ответ ставится 1 балл, при этом за каждый неверный ответ вычитается 1 балл;
- 0 баллов — не выбрано ни одного верного ответа.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- за каждое верное сопоставление ставится количество баллов, равное максимальному (2 балла), деленному на количество предлагаемых в вопросе сопоставлений;
- 0 баллов – ни одно сопоставление не выбрано верно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

II. Расчетные задачи.

1) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.