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.03 Системы обнаружения и предотвращения компьютерных атак (IDS/IPS)

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:Костин Дмитрий Владимирович, д.ф.-м.н.

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

8. Учебный год: 2027/2028 **Семестр:**7

9.Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- обучение студентов основам построения и применения систем обнаружения и предотвращения вторжений;
- обучение студентов принципам и методам защиты информации в компьютерных сетях;
- изучение средств защиты информации в информационно-аналитических системах.

Задачи учебной дисциплины:

- научиться формализовать задачу управления безопасностью информационных систем и моделировать угрозы безопасности информации;
- освоить навыки администрирования системы защиты информации от несанкционированного доступа и воздействия;
- освоить навыки администрирования систем обнаружения и предотвращения компьютерных атак.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Системы обнаружения и предотвращения компьютерных атак (IDS/IPS)» 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-1.1	Владеет средствами защиты информации в ИАС	**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-1.2	Способен администрировать системы защиты информации от несанкционированного доступа и воздействия	
		ПК-1.3	Способен администрировать системы обнаружения и предотвращения компьютерных атак	

12. Объем дисциплины в зачетных единицах/час.— 4/144.

Форма промежуточной аттестации:зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			7 семестр	
Контактная работа		100	100	
в том числе:	лекции	50	50	

	практические	0	0	
	лабораторные	50	50	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		44	44	
Промежуточная аттестация				
Итого:		**144**	**144**	

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 кобеспечению защиты откомпьютерных атак	Компьютерные системы и их компоненты как объекты защиты. Угрозы безопасности и каналы их воздействия. Направления и методы защиты информации. Методика построения защищенных компьютерных систем. Организационные методы и средства защиты компьютерных систем.	
1.2	Средства выявления илокализацииуязвимостейкомпьютерных систем квоздействию угроз безопасности	Системыобнаруженияатак (IntrusionDetection Systems, IDS).	
1.3	Практика применения	Методы и средства оценки защищенности компьютерных систем. Средства контроля доступа ккомпонентам компьютерных систем. Методы и средства обеспечениябезопасности электропитаниякомпьютерных систем.Методы и средствагарантированногоуничтожения информации.Методы и средства выявления илокализации утечек информации потехническим каналам.	
2. Лабораторные занятия			
2.1	Системный подход к обеспечению защиты откомпьютерных атак	Примеры современных КС. Характеристика компонентов КС с точки зрения уязвимости к воздействию угроз безопасности.Классификация и характеристика каналов и способов воздействия угроз безопасности на КС.Направления защиты программ,данных и других компонентов КС.Классификация методов и средствзащиты информации.Средства моделирования атак и воздействия различных угроз на компоненты КС. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков. Характеристикасистемы ЗИ для сложных КС.Методика построения комплексныхсистем защиты КС.	
2.2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности	Системыобнаруженияатак (Intrusion Detection Systems, IDS).	
2.3	Практика применения	Средства моделирования атак и воздействия различных угроз на компоненты КС. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков. Методология организации	

		бесперебойного электропитания. Устройства обеспечения бесперебойного электропитания (UPS) и управления ими.Характеристика носителей истандартных способов записи/удаленияинформации. Описание техническихсредств гарантированного удаленияинформации.Инженерные СЗИ от ПЭМИН.Классификация и характеристикапассивных и активных СЗИ отПЭМИН.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практи-ческие	Лабора-торные	Самостоя-тельная работа	Всего
1	Системный подход кобеспечению защиты откомпьютерных атак	15	-	15	14	44
2	Средства выявления илокализацииуязвимостейкомпьютерных систем квоздействию угроз безопасности	10	-	10	20	40
3	Практика применения	25	-	25	10	60
	Итого:	**50**	**-**	**50**	**44**	**144**

14. Методические указания для обучающихся по освоению дисциплины:

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 44 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Системы обнаружения и предотвращения компьютерных атак (IDS/IPS)» 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.

Особое внимание обучающихся направляется на освоение способов обнаружения и предотвращения компьютерных атак.

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 «Системы обнаружения и предотвращения компьютерных атак

(IDS/IPS)»на портале «Электронный университет ВГУ»:https://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	Петровский, Алексей Игоревич. Хакинг, крэкинг и фрикинг: Секреты, описания атак, взлом и защита / А. И. Петровский .— М. : СОЛОН-Р, 2001 .— 559 с. — (Аспекты защиты) .— ISBN 5-93455-094-2 : 165.00.
2	Скудис Эд. Противостояние хакерам : Пошаговое рук. по компьютер. атакам и эффектив. защите : Пер. с англ. / Э. Скудис .— М. : ДМК-пресс, 2003 .— 507 с. : ил. — (Защита и администрирование) .— Предм. указ.: с. 502-507 .— ISBN 5-94074-170-3.

б) дополнительная литература:

№ п/п	Источник
3	Леонтьев, Виталий Петрович. Как защитить компьютер : (Вирусы, хакеры, реклама) / В. П. Леонтьев .— М. : ОЛМА-ПРЕСС образование, 2004 .— 46,[1] с. : цв. ил. — (Компьютер. Справочник пользователя) .— ISBN 5-94849-631-7, 7000 экз.
4	Мак-Клар, Стюарт. Хакинг в Web : Атаки и защиты / С. Мак-Клар, С. Шах, Ш. Шах ; Пер. с англ. Е.Н. Василенко и др.; Под ред. А.Ю. Шелестова; Авт. предисл. В.С. Бони .— М. и др. : Вильямс, 2003 .— 374 с. : ил. — Предм. указ.: с. 367-374 .— Парал. тит. л. англ. — ISBN 5-8459-0439-0.

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

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

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Лукацкий, Алексей. Обнаружение атак / А. Лукацкий .— СПб. и др. : БХВ, 2001 .— 611 с.+ CD-ROM : ил. — (Мастер. Практическое руководство) .— ISBN 5-94157-054-6 : 122.10.
2	Милославская, Наталья Георгиевна. Интрасети: доступ в Internet, защита : учебное пособие для студентов вузов, обучающихся по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» / Н.Г. Милославская, А.И. Толстой .— М. : ЮНИТИ, 2000 .— 526, [1] с. : ил., табл. — Парал. тит. л. англ. — ISBN 5-238-00134-7 : 96.71.
3	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.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель.

Перечень необходимого программного обеспечения: Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop);VisualStudioCommunity (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/);LibreOffice (GNULesserGeneralPublicLicense (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/).

Для 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	Оценочныесредства
1	Системный подход кобеспечению защиты откомпьютерных атак	ПК-1	ПК-1.1, ПК-1.2, ПК-1.3	Комплект лабораторных заданий № 1, 2
2	Средства выявления илокализацииуязвимостейкомпьютерных систем квоздействию угроз безопасности	ПК-1	ПК-1.1, ПК-1.2, ПК-1.3	Комплект лабораторных заданий № 3
3	Практика применения	ПК-1	ПК-1.1, ПК-1.2, ПК-1.3	Комплект лабораторных заданий № 4, 5, 6, 7
Промежуточная аттестация Форма контроля –зачет с оценкой				Перечень вопросов к дифференцированному 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.Примеры современных КС. Характеристика компонентов КС с точки зрения уязвимости к воздействию угроз безопасности.

2.Классификация и характеристика каналов и способов воздействия угроз безопасности на КС.

3.Направления защиты программ, данных и других компонентов КС. Классификация методов и средств защиты информации. Средства моделирования атак и воздействия различных угроз на компоненты КС. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков. Характеристика системы ЗИ для сложных КС.

4.Методика построения комплексных систем защиты КС.

5.Системыобнаруженияатак (Intrusion Detection Systems, IDS).

6.Средства моделирования атак и воздействия различных угроз на компоненты КС. Считывающие устройства. Электронные ключи. Биометрические системы контроля доступа.

Программы для создания защищенных файлов, папок, логических дисков. Методология организации бесперебойного электропитания. Устройства обеспечения бесперебойного электропитания (UPS) и управления ими. Характеристика носителей и стандартных способов записи/удаления информации. Описание технических средств гарантированного удаления информации. Инженерные СЗИ от ПЭМИН.

7.Классификация и характеристика пассивных и активных СЗИ от ПЭМИН.

Примерный перечень тем для рефератов:

- Информационная безопасность автоматизированных систем;
- Современные технологии безопасности;
- Защита в операционных системах;
- Информационные войны;
- Интрасети: доступ в Internet, защита.

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

1) знание основных понятий и методов;
2) умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений;
3) знание имеющихся ресурсов для решения задач обнаружения и предотвращения компьютерных атак для конкретной системы;
4) умение использовать стандартные пакеты программного обеспечения для решения типовых задач обнаружения и предотвращения компьютерных атак;
5) 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.

Для оценивания результатов каждой лабораторной работы используется шкала:

Критерии оценивания	Шкала оценок
Выполнено задание лабораторной работы. Программа имеет комментарии. Устный ответпо методам, используемым в лабораторной работе, соответствует разобранным на занятиях.Обучающийся дает ответы на дополнительные вопросы. Демонстрирует знание учебного материала.	«Зачтено»
Ответ не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или отсутствие их.	«Не зачтено»

20.2. Промежуточная аттестация

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

В билет включаются теоретический вопрос и задача из лабораторной работы.

Перечень вопросов к дифференцированному зачету:

№ п/п	Вопросы
1.	Основные определения и понятия компьютерных атак, их классификация и этапы реализации.
2.	Принципы построения систем обнаружения вторжения.
3.	Существующие технологии систем обнаружения атак.
4.	Повышение эффективности на основе интегрального подхода.
5.	Анализ сетевого трафика и контента.
6.	Обнаружение аномальных выбросов трафика методами кратномасштабного анализа.
7.	Методы интеллектуального анализа данных в системах обнаружения вторжения.

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

1) знание теоретических основ;
2) умение решать задачи;
3) умение работать с алгоритмами методов и информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатовна дифференцированном зачете используется **шкала*:*** «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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

Критерии оценивания	Шкала оценок
Ответ соответствует всем перечисленным выше показателям, обучающийся дает ответы на дополнительные вопросы. Демонстрирует знание учебного материала.	«Отлично»
Ответ соответствует двум или более из перечисленных показателей, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует знание учебного материала, возможно с некоторыми ошибками.	«Хорошо»
Ответ соответствует одному из перечисленных показателей, обучающийся не дает ответы на дополнительные вопросы. Демонстрирует знание учебного материала с некоторыми ошибками.	«Удовлетворительно»
Ответ не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или отсутствие их.	«Неудовлетворительно»

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	Непосредственно для защиты информации от утечек используются:	А) DLP-системы. Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	А) DLP-системы.
2	Непосредственно для	А) DLP-системы.	Б) SIEM-

	управление информацией и событиями в системе безопасности используются:	Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	системы.
3	Непосредственно для предупреждения компьютерных атак используются:	А) DLP-системы. Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	В) IPS-системы.
4	Методом предотвращения вторжений, основанным на их предварительном обнаружении по набору известных признаков, является:	А) Сигнатурный анализ. Б) Эвристический анализ. В) Поведенческий анализ. Г) Анализ сетевого трафика.	А) Сигнатурный анализ.
5	Непосредственно для защиты БД SQL может использоваться:	А) HIDS. Б) PIDS. В) VMIDS. Г) APIDS.	Г) APIDS.
6	Непосредственно для защиты виртуальных машин может использоваться:	А) HIDS. Б) PIDS. В) VMIDS. Г) APIDS.	В) VMIDS.
7	Непосредственно для защиты отдельных сетевых хостов может использоваться:	А) HIDS. Б) PIDS. В) VMIDS. Г) APIDS.	А) HIDS.
8	Целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации называется:	-	Компьютерной атакой
9	Для предотвращения компьютерных атак используются:	-	IPS-системы
10	Для обнаружения компьютерных атак используются:	-	IPS-системы

Критерии и шкалы оценивания заданий ФОС:

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;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

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

5) Задания открытого типа (число):

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

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).