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.15Системы защиты информации от несанкционированного доступа и воздействия

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. Составитель программы::Бурлуцкая Мария Шаукатовна, д.ф.-м.н., доцент

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

8. Учебный год:2028/2029 **Семестр:**А

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- раскрытие сущности и задач систем защиты информации;
- формирование у студентов знаний, умений и навыков, необходимых для построения и анализа систем защиты информации.

Задачи учебной дисциплины:

- ознакомить студентов с принципами организации и этапами разработки СЗИ;
- изучить факторы, влияющие на организацию СЗИ;
- выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию;
- определение потенциальных каналов и методов несанкционированного доступа к информации; определение возможностей несанкционированного доступа к защищаемой информации;
- ознакомиться с материально-техническим и нормативно-методическим обеспечением функционирования СЗИ;
- изучить методы и модели оценки эффективности СЗИ.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Системы защиты информации от несанкционированного доступа и воздействия» 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.

12. Объем дисциплины в зачетных единицах/час.— 3/108.

Форма промежуточной аттестации:зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			семестр А	
Контактная работа		64	64	
в том числе:	лекции	32	32	
	практические	0	0	

	лабораторные	32	32	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		44	44	
Промежуточная аттестация				
Итого:		**108**	**108**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Введение в основы компьютерных сетей.	Основные протоколы прикладного уровня стека TCP/IP. Основные протоколы транспортного, сетевого и канального уровня стека TCP/IP.	
1.2	Виды систем защиты информации. .	Принципы работы и использования систем защиты информации: Host IDS, Network IDS/IPS, Antivirus, Data Loss Prevention, Web Application Firewall, Proxy, Firewall, Vulnerability Scanner, Sandbox, SIEM. Принципы выявления атак на основе модели Cyber-KillChain. События ИБ и их анализ для выявления атак.	
1.3	Технические средства обнаружения вторжений.	Архитектура и общее описание стека технологий ELK. Изучение агентов для сбора информации с ОС Windows, Linux. Логирование ОС Windows, политики аудита.Изучение возможностей Sysmon. Изучение возможностей системы Network IDS Suricata. Принципы работы с консолью Kibana для поиска и анализа событий ИБ.	
1.4	Стадии атаки. Методы защиты на стадии	Стадии атак «Разведка», «Доставка», «Эксплуатация», «Заражение, Закрепление, Уничтожение следов». Изучение тактик и техник злоумышленника на стадии «Разведка».	
2. Лабораторные занятия			
2.1	Введение в основы компьютерных сетей.	Сетевое оборудование, принципы работы. Vlan и Vpn, принципы построения сетей. Передача пакетов на сетевом и канальном уровнях.	
2.2	Виды систем защиты информации. .	Инциденты ИБ.Способы реагирования на инциденты ИБ. Методы автоматизации выявления инцидентов ИБ	
2.3	Технические средства обнаружения вторжений.	Разработка запросов на языке Query DSL. Изучение принципов разработки панелей визуализации событий. Изучение общих принципов разворачивания инструментов для мониторинга и диагностики неисправностей.	
2.4	Стадии атаки. Методы защиты на стадии	Изучение тактик и техник злоумышленника на стадии «Разведка». Изучение возможностей инструмента Nmap. Изучение техник и инструментов нумерации информации. Методы выявления атак на стадиях. Виды эксплойтов. Тактики и техники злоумышленников при эксплуатации уязвимостей.	

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	Введение в основы компьютерных сетей.	4		4	8	16
2	Виды систем защиты информации. .	8		8	12	28
3	Технические средства обнаружения вторжений.	8		8	12	28
4	Стадии атаки. Методы защиты на стадии	12		12	12	36
	Итого:	**32**	**-**	**32**	**44**	**108**

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 защиты информации от несанкционированного доступа и воздействия» 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 практических заданий, поиск необходимых для работы материалов в Интернете.

Особое внимание обучающихся направляется на освоение необходимого в дальнейшим математического аппарата.

Вопросы лекционных и практических 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 самостоятельных/лабораторных работ) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации.

В случае необходимости перехода на дистанционный режим обученияиспользуется электронный курс «Системы защиты информации от несанкционированного доступа и воздействия»на портале «Электронный университет ВГУ»:https://edu.vsu.ru.

Там жеразмещены необходимые для усвоения курса материалы.

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

а) основная литература:

№ п/п	Источник

1.	Бабин С.А.Лаборатория хакераСанкт-Петербург: БХВ-Петербург, 2016, 240с.
2.	Щеглов А.Ю., Щеглов К.А.Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015. – 93с.
3.	Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

б) дополнительная литература:

№ п/п	Источник
4.	Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г.Грибунин, В. В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.
5.	
6.	

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

№ п/п	Ресурс
7.	Сайт математического факультета ВГУ. Раздел, на котором размещены методические издания:https://math.vsu.ru/wp/?page_id=937.
8.	ЭБС «Университетская библиотека онлайн».
9.	Электронный каталог ЗНБ ВГУ :http://www.lib.vsu.ru .
10.	Электронный университет ВГУ: https://edu.vsu.ru/course/view.php?id=19958.

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1.	Васильева, И. Н. Интеллектуальные системы защиты информации : учебное пособие / И. Н. Васильева, Д. Ю. Федоров. — СПб.: Изд-во СПбГЭУ, 2020. – 106 с.
2.	
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).

18. Материально-техническое обеспечение дисциплины:

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

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.

Перечень необходимого программного обеспечения:

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 LesserGeneralPublicLicense (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/)

Foxit Reader, браузер Mozilla Firefox, Opera или Internet.

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	Виды систем защиты информации.	ПК-1	ПК-1.2	Тест
2	Технические средства обнаружения вторжений.			Тест
3	Стадии атаки. Методы защиты на стадии			Практическая работа
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, самостоятельных работ, контрольной работы.

Примерный перечень задач для самостоятельной работы:

Для оценивания текущего контроля успеваемости и оценивания самостоятельной работы используются следующие ***показатели:***

1) знание основных понятий и методов;
2) умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений;
3) 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

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

В билет включаются теоретический вопрос и задача из примерного перечня задач для контрольной работы.

В случае посещения обучающимся всех аудиторных занятий (лекций и лабораторных занятий) и активной работы на них, успешного выполнения элементов текущей аттестации (самостоятельные работы), оценка за промежуточнуюаттестацию может быть выставлена по результатам текущих аттестаций.

Перечень вопросов к зачету:

1. Дайте определение следующим понятиям: «Защита информации», «Системы защиты информации»
2. Системы класса HIDS. Основные функции и назначение системы.
3. Системы класса NIDS. Основные функции и назначение системы. Чем IPS отличается от IDS?
4. Системы класса Antivirus. Основные функции и способы выявления ВПО.
5. Какими каналами злоумышленник может осуществить доставку ВПО внутрь защищаемого периметра? Как при этом может быть использована социальная инженерия?
6. Что такое эксплуатация уязвимостей? Какие бывают эксплойты?
7. Что такое Payload и чем он отличается от эксплойта?
8. По каким признакам можно выявить ВПО на защищаемом хосте? Какие СЗИ для этого можно использовать?
9. Как для выявления инцидентов ИБ можно использовать репутацию внешних ресурсов сети Интернет? Что такое C&C?
10. Что такое повышение привилегий? Для каких стадий характерны подобные атаки?
11. Что такое Persistence? Для каких стадий характерны подобные атаки?
12. Опишите пример способа повышения привилегий.
13. Что такое «миграция», для чего используется злоумышленниками?

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 зачете используется **шкала*:***«зачтено».

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

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

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

1) закрытые задания (тестовые):

1. **Когда информация доступна только тому, кому она предназначена, значит ей обеспечена …**

1. имитостойкость
2. конфиденциальность *
3. целостность

2. **Авторизация это …**

1. аутентификация плюс предоставление индивидуальных прав доступа *
2. система, имеющая защиту от попыток нарушения правил разграничения доступа
3. когда всякий субъект доступа действует в рамках предписанных ему полномочий

3. **Атака на систему это …**

1. это потенциально возможное происшествие, которое может быть непреднамеренным
2. реализация угрозы *
3. подтверждение того, что объект, участвующий во взаимодействии, является тем, за кого себя выдает

4. **Конфиденциальность информации достигается путем использования …**

1. специальных каналов *
2. авторизации
3. полной подконтрольности и подотчетности действий оператора

5. **Сетевые атаки осуществляются …**

1. в пределах локальной КС
2. из-за пределов локальной КС *
3. непосредственно в локальной КС

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).