Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____ Галкин А. А.
«_26_» _августа_ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность информационных систем
(наименование дисциплины)

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Безопасность информационных систем» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность». Целью освоения дисциплины является формирование теоретических знаний и практических навыков по обеспечению информационной безопасности информационных систем.

Задачей изучения дисциплины является освоение принципов и основных подходов к обеспечению безопасного функционирования различных механизмов информационной безопасности в информационных системах. Кроме того, в данном курсе изучаются вопросы безопасного использования современных информационных технологий при эксплуатации автоматизированных информационных систем с целью формирования навыков противодействия несанкционированному проникновению в защищаемые информационные системы с использованием современных информационно-вычислительных средств и систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность информационных систем» относится к обязательным дисциплинам обязательной части Блока Б1 (код Б1.О.03) направления подготовки 10.03.01 «Информационная безопасность». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ, практических занятий и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1.1.	Знать эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы	Тестовые вопросы
	ОПК-2.1.2.	Знать основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-2.1.3.	Знать защитные механизмы и средства обеспечения безопасности операционных систем	
	ОПК-2.1.4.	Знать средства и методы хранения и передачи аутентификационной информации	
	ОПК-2.1.5.	Знать требования к подсистеме аудита и политике аудита	
	ОПК-2.1.6.	Знать принципы построения современных операционных систем и особенности их применения	
	ОПК-2.2.1.	Уметь выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	

	ОПК-2.2.2.	формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе	
	ОПК-2.2.3.	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
	ОПК-2.2.4.	Уметь применять основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-2.2.5.	Уметь основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоко	
	ОПК-2.2.6.	Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	
	ОПК-2.3.1.	Владеть навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	
	ОПК-2.3.2.	Владеть навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств	
	ОПК-2.3.3.	Владеть навыками конфигурирования и администрирования операционных систем	
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1.	Знать основные виды политик управления доступом и информационными потоками в компьютерных системах	Тестовые вопросы
	ОПК-10.1.2.	Знать защитные механизмы и средства обеспечения безопасности операционных систем	
	ОПК-10.1.3.	Знать средства и методы хранения и передачи аутентификацион. информации	
	ОПК-10.1.4.	Знать требования к подсистеме аудита и политике аудита	
	ОПК-10.2.1.	Уметь формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе	
	ОПК-10.2.2.	Уметь применять основные виды политик управления доступом и информационными потоками в компьютерных системах	
	ОПК-10.2.3.	Уметь основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков	
	ОПК-10.2.4.	Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	

	ОПК-10.3.1.	Владеть навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	
	ОПК-10.3.2.	Владеть навыками конфигурирования и администрирования операционных систем	
ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2 -1.1	Знать средства, методы и протоколы идентификации, аутентификации и авторизации	Тестовые вопросы
	ОПК-4.2 -2.1	Уметь устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации;	
	ОПК-4.2 -2.2	Уметь управлять полномочиями пользователей	
	ОПК-4.2 -3.1	Владеть навыками конфигурирования и администрирования операционных систем	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 8 зачетных единиц, 288 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Цели и задачи дисциплины. Методики и программные средства идентификации	4	1-2	4				10	
2	Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.	4	3-4	4		4		10	
3	Методики и программные средства идентификации сетевых служб на узлах корпоративной сети	4	5-6	4				10	Рейтинг-контроль №1
4	Методики и программные средства идентификации операционных систем на узлах корпоративной сети	4	7-8	4		4		10	
5	Методы и программные средства обнаружения открытых портов узла сети.	4	9-10	4				10	

6	Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.	4	11-12	4		4		10	Рейтинг-контроль №2
7	Методики и программные средства построения сетевых диаграмм КИС.	4	13-14	4				10	
8	Инвентаризация ресурсов КИС. Подходы и методики. Применение специальных сетевых протоколов для инвентаризации ресурсов КИС	4	15-16	4		4		10	
9	Особенности анализа сетевого трафика в коммутируемой среде	4	17-18	4		2		10	Рейтинг-контроль №3
Всего за 4 семестр:		**144**		**36**		**18**		**90**	**Зачет**
10	Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде	5	1-2	4	4	4		4	
11	Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.	5	3-4	4	4	4		4	
12	Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning	5	5-6	4	4	4		4	Рейтинг-контроль №1
13	Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing	5	7-8	4	4	4		4	
14	Sniffing атаки в коммутируемой сетевой среде	5	9-10	4	4	4		4	
15	Сканеры уязвимостей и методики их применения. Особенности применения сканера OpenVAS	5	11-12	4	4	4		4	Рейтинг-контроль №2
16	Программные средства анализа защищенности WEB приложений. Services fingerprinting. Программные инструменты Services fingerprinting.	5	13-14	4	4	4		4	
17	OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing	5	15-16	4	4	4		4	
18	OS Fingerprinting. Пассивное и активное исследование стека в задаче идентификации ОС	5	17-18	4	4	4		4	Рейтинг-контроль №3
Всего за 5 семестр:		**144**		**36**	**36**	**36**		**36**	**Зачет с оценкой**
Наличие в дисциплине КП/КР		**НЕТ**							
Итого по дисциплине		**288**		**72**	**36**	**54**		**126**	**Зачет; Зачет с оценкой**

Содержание лекционных занятий по дисциплине 4 семестр

Темы 1-2. Цели и задачи дисциплины. Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.

Темы 3-4. Сетевая разведка. Методы сканирования корпоративной сети. Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.

Темы 5-6. Методы сканирования корпоративной сети. Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.

Темы 7-8. Методы сканирования корпоративной сети. Методики и программные средства идентификации операционных систем на узлах корпоративной сети.

Темы 9-10. Методы сканирования корпоративной сети. Методы и программные средства обнаружения открытых портов узла сети.

Темы 11-12. Методы сканирования корпоративной сети. Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.

Темы 13-14. Анализ сетевого трафика. Методики и программные средства построения сетевых диаграмм КИС. Инвентаризация ресурсов Linux узлов КИС. Анализ сетевого трафика. Инвентаризация ресурсов Windows узлов КИС.

Темы 15-16. Анализ сетевого трафика. Инвентаризация ресурсов КИС. Подходы и методики. Применение специальных сетевых протоколов для инвентаризации ресурсов КИС

Темы 17-18. Анализ сетевого трафика. Особенности анализа сетевого трафика в коммутируемой среде.

Содержание лекционных занятий по дисциплине 5 семестр

Темы 1-2. Атаки на КИС. Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.

Темы 3-4. Атаки на КИС. Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.

Тема 5-6. Атаки на КИС. Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning.

Тема 7-8. Атаки на КИС. Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.

Тема 9-10. Атаки на КИС. Sniffing атаки в коммутируемой сетевой среде.

Тема 11-12. Сканеры уязвимостей и методики их применения. Особенности применения сканера OpenVAS.

Тема 13-14. Программные средства анализа защищенности баз данных. Программные средства анализа защищенности WEB приложений. Services fingerprinting. Программные инструменты Services fingerprinting.

Тема 15-16. OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.

Тема 17-18. OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС. Активное исследование стека в задаче идентификации ОС

Содержание лабораторных занятий по дисциплине
4 семестр

Лабораторная работа №1. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Лабораторная работа №2. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения

Лабораторная работа №3. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)

Лабораторная работа №4. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP.

Содержание лабораторных занятий по дисциплине
5 семестр

Лабораторная работа №1. Специализированные программные средства активного исследования стека TCP/IP

Лабораторная работа №2. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)

Лабораторная работа №3. Специальное ПО анализа уязвимостей OpenVas. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)

Лабораторная работа №4. Программные средства анализа защищенности баз данных.

Лабораторная работа №5. Программные средства анализа защищенности WEB приложений

Лабораторная работа №6. OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.

Лабораторная работа №7. OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС

Лабораторная работа №7. OS Fingerprinting. Активное исследование стека в задаче идентификации ОС

Содержание практических занятий по дисциплине
5 семестр

Практическое занятие №1. Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.

Практическое занятие №2. Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning

Практическое занятие №3. Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing

Практическое занятие №4. Sniffing атаки в коммутируемой сетевой среде

Практическое занятие №5. Сканеры уязвимостей и методики их применения

Практическое занятие №6. Программные средства анализа защищенности баз данных

Практическое занятие №7. Программные средства анализа защищенности WEB приложений

Практическое занятие №7. Программные инструменты Services fingerprinting

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Вопросы рейтинг-контроля №1 семестр 4:

- Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
- Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.
- Методики и программные средства идентификации операционных систем на узлах корпоративной сети.
- Сканирование сети. Методы и программные средства обнаружения открытых портов узла сети.
- Сканирование сети. Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.

Вопросы рейтинг-контроля №2 семестр 4:

- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Сканирование сети. Тип сканирования Full Open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Half-open Scan. Особенности использования рассматриваемого типа сканирования.

- Сканирование сети. Тип сканирования Xmas Tree Scan. Особенности использования рассматриваемого типа сканирования.

Вопросы рейтинг-контроля №3 семестр 4:

- Сканирование сети. Тип сканирования FIN Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования NULL Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ACK Scanning. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ARP Scan. Особенности использования рассматриваемого типа сканирования.
- Services fingerprinting. Основные понятия.
- Services fingerprinting. Методы Services fingerprinting.
- Построение карты сети. Программные средства Drawing Network Diagrams.
- Enumeration. Понятие, цели и задачи Enumeration.

Вопросы рейтинг-контроля №1 семестр 5:

- Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.
- Атаки DOS. Цели и задачи атак DOS.
- Атаки DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods.
- Атаки DOS. SYN Attack/Flood.
- Атаки DOS. ICMP Flood Attack.
- Атаки DOS. Программные средства проведения атак.
- Атаки DOS. Ping of Death.
- Атаки DOS. Teardrop.
- Атаки DOS. Smurf. Атаки DOS. Fraggle.
- Атаки DOS. Программные средства проведения атак.
- Атаки Buffer Overflow.
- Атаки DDOS. Особенности реализации.

Вопросы рейтинг-контроля №2 семестр 5:

- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- OpenVAS. Методика сканирования.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Анализ DNS.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Обнаружение активных узлов сети.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Идентификация сетевых служб и операционной системы узлов сети.
- Программные средства обнаружения IDS в корпоративной сети.
- Атаки на протоколы удаленного управления устройствами КИС.

Вопросы рейтинг-контроля №3 семестр 5:

- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к зачету 4 семестр

- Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
- Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.
- Методики и программные средства идентификации операционных систем на узлах корпоративной сети.
- Сканирование сети. Методы и программные средства обнаружения открытых портов узла сети.
- Сканирование сети. Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.
- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Сканирование сети. Тип сканирования Full Open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Half-open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Xmas Tree Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования FIN Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования NULL Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ACK Scanning. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ARP Scan. Особенности использования рассматриваемого типа сканирования.
- Services fingerprinting. Основные понятия.
- Services fingerprinting. Методы Services fingerprinting.
- Построение карты сети. Программные средства Drawing Network Diagrams.
- Enumeration. Понятие, цели и задачи Enumeration.

Примерный перечень вопросов к зачету 5 семестр

- Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.
- Атаки DOS. Цели и задачи атак DOS.
- Атаки DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods.
- Атаки DOS. SYN Attack/Flood.
- Атаки DOS. ICMP Flood Attack.

- Атаки DOS. Программные средства проведения атак.
- Атаки DOS. Ping of Death.
- Атаки DOS. Teardrop.
- Атаки DOS. Smurf. Атаки DOS. Fraggle.
- Атаки DOS. Программные средства проведения атак.
- Атаки Buffer Overflow.
- Атаки DDOS. Особенности реализации.
- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- OpenVAS. Методика сканирования.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Анализ DNS.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Обнаружение активных узлов сети.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Идентификация сетевых служб и операционной системы узлов сети.
- Программные средства обнаружения IDS в корпоративной сети.
- Атаки на протоколы удаленного управления устройствами КИС.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов 4 семестр

- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting.
- Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Сканирование сети. Тип сканирования Full Open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Half-open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Xmas Tree Scan. Особенности использования рассматриваемого типа сканирования.

• Сканирование сети. Тип сканирования FIN Scan. Особенности использования рассматриваемого типа сканирования.
• Сканирование сети. Тип сканирования NULL Scan. Особенности использования рассматриваемого типа сканирования.
• Сканирование сети. Тип сканирования ACK Scanning. Особенности использования рассматриваемого типа сканирования.
• Сканирование сети. Тип сканирования ARP Scan. Особенности использования рассматриваемого типа сканирования.
• Services fingerprinting. Основные понятия.
• Services fingerprinting. Методы Services fingerprinting.
• Построение карты сети. Программные средства Drawing Network Diagrams.
• Enumeration. Понятие, цели и задачи Enumeration.
• Enumeration. Инвентаризация ресурсов OS Windows. Методы и средства.

Примерные вопросы и задания для самостоятельной работы студентов 5 семестр
• Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.
• Атаки DOS. Цели и задачи атак DOS.
• Атаки DOS. Типы атак DOS.
• Атаки DOS. Service Request Floods.
• Атаки DOS. SYN Attack/Flood.
• Атаки DOS. ICMP Flood Attack.
• Атаки DOS. Программные средства проведения атак.
• Атаки DOS. Ping of Death.
• Атаки DOS. Teardrop.
• Атаки DOS. Smurf. Атаки DOS. Fraggle.
• Атаки DOS. Программные средства проведения атак.
• Атаки Buffer Overflow. Принципы.
• Атаки DDOS. Особенности реализации.
• Беспроводные сети. Угрозы и уязвимости Wireless Networks.
• Беспроводные сети. Аутентификация Wi-fi.
• Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
• Сканеры уязвимостей. Идентификация уязвимостей в сетях.
• OpenVAS. Методика сканирования.
• Сканеры уязвимостей. Уязвимости БД.
• Средства анализа защищенности БД.
• Сканеры уязвимостей. Уязвимости WEB приложений.
• Средства анализа защищенности WEB приложений.
• Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Анализ DNS.
• Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Обнаружение активных узлов сети.
• Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Идентификация сетевых служб и операционной системы узлов сети.
• Программные средства обнаружения IDS в корпоративной сети.
• Атаки на протоколы удаленного управления устройствами КИС.
• Распределенные атаки DDOS в корпоративной сетевой среде.
• Моделирование атак DDOS в корпоративной сетевой среде.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
Технологии обеспечения безопасности информационных систем: учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва; Берлин: Директ-Медиа, 2021. – 210 с.– DOI 10.23681/598988	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 11.09.2021)
Брюхомицкий, Ю. А. Безопасность информационных технологий: учебное пособие: в 2 частях: [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – Ч. 1. – 171 с. - ISBN 978-5-9275-3526-2	2020	https://biblioclub.ru/index.php?page=book&id=612167 (дата обращения: 11.09.2021)
Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие: [16+] / А. М. Голиков; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с.	2015	https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 11.09.2021)
Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с. DOI 10.23681/571485	2020	https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 11.09.2021)
Дополнительная литература		
Кияев, В. Безопасность информационных систем: курс: [16+] / В. Кияев, О. Граничин. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.	2016	https://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 11.09.2021)
Организация безопасной работы информационных систем: учебное пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др.;– Тамбов: Тамбовский государственный технический университет (ТГТУ), 2014. – 132 с.	2014	https://biblioclub.ru/index.php?page=book&id=277794 (дата обращения: 11.09.2021)
Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений: учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва; Берлин: Директ-Медиа, 2021. – 175 с. – DOI 10.23681/599050	2021	https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 11.09.2021)
Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. – DOI 10.23681/276557	2015	https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 11.09.2021)

6.2. Периодические издания

1.«Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;

2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

6.3. Интернет-ресурсы

1. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
2. ИНТУИТ. Национальный открытый университет. – Режим доступа: http://www.intuit.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил:
старший преподаватель кафедры ИЗИ Матвеева А.П._____

Рецензент: Заместитель руководителя РАЦ ООО
«ИнфоЦентр» к.т.н. Вертилевский Н.В_____

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.04.21 года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»

Протокол № 1 от 26.04.21 года
Председатель комиссии д.т.н., профессор_____/М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 2022 / 2023 учебный год
Протокол заседания кафедры № 14 от 28.06.22 года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный годаПротокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год
Протокол заседания кафедры № _____ от _____ года

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Безопасность информационных систем

образовательной программы направления подготовки *10.03.01 Информационная безопасность*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/__

Подпись *ФИО*