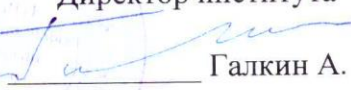


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

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

10.05.04 «Информационно-аналитические системы безопасности»

(код и наименование направления подготовки (специальности))

направленность (профиль) подготовки

Автоматизация информационно-аналитической 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 специальности 10.05.04 «Информационно-аналитические системы безопасности». 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 обязательной части Блока Б1 (код Б1.О.04) учебного плана специальности 10.05.04 «Информационно-аналитические системы безопасности». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ 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-6 Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности	ОПК-6.1.1	Знать активные и пассивные методы сбора информации	Тестовые вопросы
	ОПК-6.1.2	Знать информационные технологии в системе информационно-аналитического обеспечения безопасности	
	ОПК-6.1.3	Знать механизмы реализации атак в компьютерных сетях	
	ОПК-6.1.4	Знать защитные механизмы и средства обеспечения сетевой безопасности	
	ОПК-6.1.5	Знать основные методы организационного обеспечения информационной безопасности специальных АИС	
	ОПК-6.1.6	Знать методологические основы, методы и средства построения распределенных специальных АИС	
	ОПК-6.1.7	Знать нормативную базу, регламентирующую создание и эксплуатацию специальных АИС	
	ОПК-6.2.1	Уметь решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных	

Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2.2	Уметь проектировать и сопровождать типовые специальные АИС	
	ОПК-6.2.3	Уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях	
	ОПК-6.2.4	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
	ОПК-6.2.5	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками	
	ОПК-6.3.1	Владеть навыками работы с имеющимися на рынке информационно-аналитическими системами	
	ОПК-6.3.2	Владеть навыками обработки информации в специальных АИС	
	ОПК-6.3.3	Владеть навыками выбора и обоснования критериев эффективности функционирования специальных АИС	
	ОПК-6.3.4	Владеть навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств	
	ОПК-6.3.5	Владеть методами и средствами выявления угроз безопасности компьютерным системам	
ОПК-13 Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.1.1	Знать принципы организации информационных систем в соответствии с требованиями по защите информации	Тестовые вопросы
	ОПК-13.1.2	Знать основные этапы процесса проектирования и общие требования к содержанию проекта	
	ОПК-13.2.1	Уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
	ОПК-13.2.2	Уметь анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
	ОПК-13.2.3	Уметь формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения	
	ОПК-13.3.1	Владеть методами и средствами выявления угроз безопасности компьютерным системам	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 16 зачетных единиц, 576 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 и (по неделям семестра), форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	В форме прак. подготовок		
1.	Сетевая разведка. Первичный сбор информации о КИС	4	1-6	12		6		27	Рейтинг-контроль №1
2.	Методологии Penetration Testing.	4	7-12	12		6		27	Рейтинг-контроль №2
3.	Методики сканирования сетей	4	13-18	12		6		27	Рейтинг-контроль №3
Всего за 4 семестр:			180	36		18		81	Экзамен 45
4.	Инвентаризация ресурсов КИС	5	1-5	9		9		20	Рейтинг-контроль №1
5.	Атаки типа отказ в обслуживании на ресурсы КИС	5	6-9	9		9		21	
6.	Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде	5	10-13	9		9		20	Рейтинг-контроль №2
7.	Атаки типа отказ в обслуживании на ресурсы КИС.	5	14-18	9		9		20	Рейтинг-контроль №3
Всего за 5 семестр:			180	36		36		81	Экзамен 27
8.	Методики анализа защищенности беспроводной сети КИС	6	1-6	6		12		39	Рейтинг-контроль №1
9.	Методики анализа защищенности WEB приложений и БД.	6	7-12	6		12		39	Рейтинг-контроль №2
10.	Стандарты тестирования на проникновение	6	13-18	6		12		39	Рейтинг-контроль №3
Всего за 6 семестр:			216	18		36		117	Экзамен 45
Наличие в дисциплине КП/КР			Есть(6)						
Итого по дисциплине			576	90		90		279	Экзамен 45 Экзамен 27 Экзамен 45 Курсовая работа

Содержание лекционных занятий по дисциплине

Раздел 1. Введение

Тема 1. Цели и задачи дисциплины.

Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.

Тема 2. Сетевая разведка

Методы сканирования корпоративной сети. Методики и программные средства идентификации операционных систем на узлах корпоративной сети. Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.

Раздел 2. Анализ сетевого трафика.

Тема 1. КИС

Методики и программные средства построения сетевых диаграмм КИС. Инвентаризация ресурсов Linux узлов КИС. Инвентаризация ресурсов Windows узлов КИС. Инвентаризация ресурсов КИС. Подходы и методики.

Тема 2. Методики анализа

Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде. Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.

Раздел 3. Атаки

Тема 1. Типы атак

Атаки типа отказ в обслуживании на ресурсы КИС. Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС. Атаки на беспроводные сети КИС.

Тема 2. Защита

Особенности применения сканера OpenVAS. Программные средства анализа защищенности баз данных. Программные средства анализа защищенности WEB приложений.

Содержание лабораторных занятий по дисциплине

Раздел 1. Введение

Тема 1. Цели и задачи дисциплины.

Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Тема 2. Сетевая разведка

Обнаружение узлов корпоративной сети. Информационные ICMP сообщения

Раздел 2. Анализ сетевого трафика.

Тема 1. КИС

Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)

Тема 2. Методики анализа

Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP. Специализированные программные средства активного исследования стека TCP/IP

Раздел 3. Атаки

Тема 1. Типы атак

Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)

Тема 2. Защита

Специальное ПО анализа уязвимостей OpenVas. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)

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.
- Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.
- Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде.

Вопросы рейтинг-контроля №3 семестр 4:

- 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.

Вопросы рейтинг-контроля №1 семестр 5:

- Методологии Penetration Testing.
- Понятие Footprinting. Этапы.
- Методы сканирования корпоративной сети.
- Методики и программные средства обнаружения активных узлов корпоративной сети.

- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети.
- Сканирование сети. Методы и программные средства сканирования сети.
- Сканирование сети. Обнаружение открытых портов узла сети.

Вопросы рейтинг-контроля №2 семестр 5:

- Методики и программные средства построения сетевых диаграмм КИС.
- Инвентаризация ресурсов КИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов КИС.
- Инвентаризация ресурсов Windows узлов КИС.
- Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.

Вопросы рейтинг-контроля №3 семестр 5:

- Атаки типа отказ в обслуживании на ресурсы КИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
- Атаки на беспроводные сети КИС.
- Программные средства проведения атак на беспроводные сети КИС. • __ Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Анализ трафика.
- Программные инструменты специального дистрибутива KALI Linux для стресс тестирования КИС.
- Методики обнаружения межсетевых экранов в корпоративной сети.
- Программные средства обнаружения межсетевых экранов в корпоративной сети.
- Методики обнаружения IDS в корпоративной сети.

Вопросы рейтинг-контроля №1 семестр 6:

- 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

Вопросы рейтинг-контроля №2 семестр 6:

- 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.

Вопросы рейтинг-контроля №3 семестр 6:

- 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.
- Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Перечень вопросов к зачету 4 семестр (промежуточной аттестации по итогам освоения дисциплины):

- 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.
- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.
- Сканирование сети. Методы и программные средства обнаружения открытых портов узла сети.
- Сканирование сети. Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.
- Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде.
- 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.

Перечень вопросов к экзамену 5 семестр (промежуточной аттестации по итогам освоения дисциплины):

- Методологии Penetration Testing.
- Понятие Footprinting. Этапы.
- Методы сканирования корпоративной сети.
- Методики и программные средства обнаружения активных узлов корпоративной сети.

- Методики и программные средства построения сетевых диаграмм КИС.
- Инвентаризация ресурсов КИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов КИС.
- Инвентаризация ресурсов Windows узлов КИС.
- Атаки типа отказ в обслуживании на ресурсы КИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
- Атаки на беспроводные сети КИС.
- Программные средства проведения атак на беспроводные сети КИС.
- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети.
- Сканирование сети. Методы и программные средства сканирования сети.
- Сканирование сети. Обнаружение открытых портов узла сети.
- Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Анализ трафика.
- Программные инструменты специального дистрибутива KALI Linux для стресс тестирования КИС.
- Методики обнаружения межсетевых экранов в корпоративной сети.
- Программные средства обнаружения межсетевых экранов в корпоративной сети.
- Методики обнаружения IDS в корпоративной сети.

Перечень вопросов к экзамену 6 семестр (промежуточной аттестации по итогам освоения дисциплины):

- 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
- 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.
- 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.
- Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.

5.3. Самостоятельная работа обучающегося.

- 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.
- 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.
- 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. Белокопской, 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 «Пирания-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 Chaos), 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 26.09.21 года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии
специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № 1 от 26.09.21 года
Председатель комиссии д.т.н., профессор _____ /М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год
Протокол заседания кафедры № 14 от 28.06.21 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 года
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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
в рабочую программу дисциплины *Безопасность информационных систем*
образовательной программы специальности
10.05.04 «Информационно-аналитические системы безопасности»

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