



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01.12 Администрирование средств защиты информации в
компьютерных системах и сетях

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): *бакалавр*

Форма обучения: *очная*

Институт: математики естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	4		
Семестр/триместр	7,8		

Лекции	26		
Лабораторные занятия	36		
Практические (семинарские) занятия	36		
в т. ч. практическая подготовка	8		
Форма(ы) промежуточной аттестации	Зачет (7 семестр) Экзамен - 0.3 (8 семестр)		
Контроль	9		
Иные формы работы			
Самостоятельная работа	36,7		

Всего часов: 144

Трудоемкость: 4 зачетных единиц.

Разработчик(и) рабочей программы:

к.т.н., доцент А.А. Петров, ассистент Д.Д. Маторин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

ознакомление обучающихся с методами организации защиты конфиденциальных данных от непреднамеренных ошибок, основными методами информационной безопасности и средствами защиты компьютерной информации, законодательством и стандартами в этой области.

Задачи изучения дисциплины:

- освоение обучающимися основных положений теории информационной безопасности в компьютерных системах;
- освоение обучающимися основных принципов и методов, применяемых при защите компьютерных систем;
- изучение правовых основ защиты информации в компьютерной системе;
- изучение организационно-технических, программно-аппаратных методов и средств защиты информации;
- изучение стандартов, моделей и методов шифрования информации, методов идентификации пользователей, методов защиты программ от вирусов;
- оценка защищенности компьютерных систем.

Место дисциплины в структуре ОПОП: реализуется в рамках части, формируемой участниками образовательных отношений блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПКС-1	Знать: - сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению; - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.	Знает: - основные средства защиты информации в компьютерных системах и сетях и принципы их работы; - основные принципы и методы защиты информации в компьютерных сетях, методы поиска информации. - основы администрирования средства защиты информации в компьютерных системах и сетях.
	Уметь: - оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы	Умеет: - формировать политику информационной безопасности; - подбирать меры по обеспечению информационной безопасности на объекте защиты. - выявлять угрозы информации в

	защиты информации; - принимать управленческие и административные решения в сфере защиты информации.	компьютерных сетях.
	Владеть: категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации; - правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.	Владеет: - навыками поиска запрещенного контента в сети, администрирования программно-аппаратных средств и обеспечения необходимого уровня защиты информации в компьютерных сетях; - навыками администрирования средств защиты информации и управления процессом реализации комплекса мер по обеспечению информационной безопасности.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
Раздел 1. Защищенность операционной системы		72	10	20	20	22
1.	Тема 1. Методы создания защищенных информационных систем	14	2	4	4	4
2.	Тема 2. Теоретические основы защиты ОС. Стандарты защищенности. Формальное представление политик безопасности	14	2	4	4	4
3.	Тема 3. Методы защиты операционных систем. Структура безопасной операционной системы	14	2	4	4	4
4.	Тема 4. Конфигурирование безопасной загрузки Механизмы загрузки Windows NT	14	2	4	4	4
5.	Тема 5. Реализация механизмов защиты в операционных системах. Структура и состав подсистем безопасности. Контроль многопользовательского доступа. Механизмы аутентификации.	16	2	4	4	6
	контроль					
	консультация					
	зачет					
	итого за 7 семестр	72	10	20	20	22

	<i>в т.ч. практическая подготовка</i>	2				
	<i>в т.ч. лабораторная подготовка</i>	2				
Раздел 2. Администрирование локальной безопасности		62,7	16	16	16	14,7
6.	Тема 6. Управление учетными записями пользователей и групп. Политики учетных записей. Аудит и журналирование событий безопасности	8	2	2	2	2
7.	Тема 7. Командный режим управления. Символические имена и маски. Перенаправление информационного потока. Базовые, сервисные и информационные команды	8	2	2	2	2
8.	Тема 8. Автоматизация администрирования . Язык сценариев. Командные файлы. Параметры запуска, переменные и операции над ними. Реализация разветвлений и циклов в сценариях	14	4	4	4	2
9.	Тема 9. Мониторинг производительности и процессов	16	4	4	4	4
10.	Тема 10. Планирование и управление заданиями	16,7	4	4	4	4,7
	<i>контроль</i>	9				
	<i>консультация</i>					
	<i>экзамен</i>	0,3				
Итого за 8 семестр		62,7	16	16	16	14,7
	<i>в т.ч. практическая подготовка</i>	2				
	<i>в т.ч. лабораторная подготовка</i>	2				
ИТОГО:		144	26	36	36	36,7

Очно-заочная форма обучения (не реализуется)

Заочная форма обучения (не реализуется)

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме теста, реферата.

Примерный вариант учебно-контрольного теста

1. **Что из перечисленного относится к основным принципам информационной безопасности?**
 - a) Доступность, конфиденциальность, целостность
 - b) Политика доступа, контроль, безопасность
 - c) Шифрование, хеширование, аутентификация
 - d) Сеть, оборудование, ПО
2. **Что такое аутентификация?**
 - a) Процесс передачи данных
 - b) Процесс подтверждения личности пользователя
 - c) Процесс шифрования информации
 - d) Процесс восстановления данных
3. **Какой из методов шифрования является симметричным?**
 - a) RSA
 - b) AES
 - c) ECC
 - d) DSA
4. **Какой компонент отвечает за разграничение доступа к ресурсам системы?**
 - a) Система резервного копирования
 - b) Межсетевой экран (Firewall)
 - c) Антивирусная система
 - d) Система управления доступом (Access Control)
5. **Что такое политика безопасности?**
 - a) Набор программ для защиты данных
 - b) Систематизированный свод правил и инструкций по защите информации
 - c) Методика шифрования данных
 - d) Протокол для обеспечения безопасности сети
6. **Какая из систем контроля доступа к данным является наиболее распространённой?**
 - a) DAC (Discretionary Access Control)
 - b) MAC (Mandatory Access Control)
 - c) RBAC (Role-Based Access Control)
 - d) ABAC (Attribute-Based Access Control)
7. **Какую роль выполняет межсетевой экран (Firewall)?**
 - a) Обнаружение вредоносного ПО
 - b) Контроль и фильтрация входящего и исходящего трафика
 - c) Шифрование данных в сети
 - d) Анализ уязвимостей программного обеспечения
8. **Какая функция системы IDS (Intrusion Detection System)?**
 - a) Оповещение о несанкционированных попытках проникновения в систему
 - b) Автоматическое восстановление данных
 - c) Управление доступом к файлам
 - d) Шифрование сетевого трафика
9. **Какая команда используется для управления брандмауэром в Linux (iptables)?**
 - a) ipsec
 - b) iproute2
 - c) iptables
 - d) netstat
10. **Какой инструмент мониторинга сети чаще всего используется для анализа трафика?**
 - a) Nmap

- b) Wireshark
 - c) Nessus
 - d) OpenVAS
11. **Что из перечисленного является первым шагом в реагировании на инцидент безопасности?**
- a) Обнаружение и идентификация инцидента
 - b) Восстановление системы
 - c) Оповещение пользователей
 - d) Анализ журналов системы
12. **Какой метод используется для защиты данных при передаче через незащищённые каналы?**
- a) VPN
 - b) DNS
 - c) HTTP
 - d) DHCP

Примерная тематика рефератов

1. Современные угрозы информационной безопасности и методы защиты.
2. Основные модели контроля доступа: сравнение и области применения.
3. Криптографические методы защиты информации.
4. Межсетевые экраны (Firewall): роль в защите корпоративных сетей.
5. Системы обнаружения и предотвращения вторжений (IDS/IPS) в корпоративных сетях.
6. SSL/TLS и IPsec: протоколы защиты сетевых соединений.
7. Социальная инженерия и её роль в кибератаках.
8. Этичный хакинг и тестирование на проникновение.
9. Облачные технологии и защита данных в облачных инфраструктурах.
10. Управление инцидентами информационной безопасности в корпоративной среде.
11. Безопасность виртуальных машин и сред виртуализации.
12. Стратегии резервного копирования и восстановления данных.
13. Антивирусные программы: принципы работы и их роль в защите информации.
14. DDoS-атаки: методы защиты и минимизации ущерба.
15. Информационная безопасность в малых и средних предприятиях: подходы и решения.
16. Протоколы и методы шифрования электронной почты.
17. Защита беспроводных сетей: Wi-Fi и технологии безопасности.

Промежуточная аттестация обучающихся осуществляется в форме зачета, экзамена, с использованием следующих оценочных материалов: перечень вопросов к зачету, экзамену.

Вопросы к зачету (7 семестр, очная форма обучения)

1. Основные принципы информационной безопасности.
2. Виды угроз информационной безопасности.
3. Различия между симметричным и асимметричным шифрованием.
4. Методы аутентификации и их примеры.

5. Что такое многофакторная аутентификация?
6. Описание моделей контроля доступа (DAC, MAC, RBAC).
7. Понятие политики безопасности и её разработка.
8. Роль межсетевого экрана (Firewall) в защите сети.
9. Принцип работы IDS и IPS.
10. Протоколы защиты данных: SSL/TLS, IPsec, VPN.
11. Задачи антивирусных программ.
12. Что такое хеширование и его использование.
13. Основы защиты виртуальных машин и облаков.
14. Встроенные механизмы защиты операционных систем.
15. Как защищаются файловые системы и данные?
16. Процесс управления инцидентами информационной безопасности.
17. Методы анализа журналов (логов).
18. Настройка межсетевого экрана (пример правил).
19. Инструменты мониторинга сетевого трафика.
20. Роль этичного хакинга и тестирования на проникновение.
21. Стратегии резервного копирования и их важность.

Вопросы к экзамену (8 семестр, очная форма обучения)

1. Основные принципы информационной безопасности.
2. Методы аутентификации и авторизации.
3. Симметричное и асимметричное шифрование.
4. Модели контроля доступа: DAC, MAC, RBAC.
5. Типы и функции межсетевых экранов.
6. Различия между IDS и IPS.
7. Политика безопасности. Основные элементы.
8. Протоколы безопасности: SSL/TLS, IPsec.
9. Этапы управления инцидентами безопасности.
10. Настройка правил межсетевого экрана.
11. Инструменты для мониторинга сетевого трафика (Wireshark, Nmap).
12. Встроенные механизмы защиты операционных систем.
13. Защита виртуальных машин и облачных сервисов.
14. Стратегии резервного копирования данных.
15. Тестирование на проникновение: цели и инструменты.
16. Шифрование данных на уровне файловой системы и сети.
17. Защита от DDoS-атак: методы и инструменты.
18. Анализ системных логов для обнаружения угроз.
19. Защита мобильных устройств в корпоративной среде.
20. Действия при утечке данных.
21. Реализация политики доступа к конфиденциальной информации.
22. Анализ и устранение сетевых уязвимостей.

23. Ответ на кибератаку: шаги восстановления.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Аверченков, В. И. Аудит информационной безопасности: учебное пособие: [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 269 с.: ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=93245> (дата обращения: 18.04.2024). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст: электронный.

4.2. Дополнительная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539995> (дата обращения: 18.04.2024).
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/538066> (дата обращения: 18.04.2024).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	https://infourok.ru/	Инфоурок: образовательный интернет-проект России. Включает: конспекты уроков, презентации, тесты, видеоуроки и другие материалы по предметам школьной программы.	Свободный доступ
2.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- LibreOffice и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия проводятся в специализированных лабораториях, оснащенных автоматизированными рабочими местами с компьютерами.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.