

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Колледж

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

по программе подготовки специалистов среднего звена (ППССЗ) среднего
профессионального образования

Специальность:	<i>10.02.05. Обеспечение информационной безопасности автоматизированных систем</i>
Обучение:	<i>по программе базовой подготовки</i>
Уровень образования, на базе которого осваивается ППССЗ:	<i>среднее общее образование</i>
Квалификация:	<i>техник по защите информации</i>
Форма обучения:	<i>очная</i>

Рабочая программа дисциплины «Корпоративная защита от внутренних угроз информационной безопасности» разработана на основе требований Федерального государственного образовательного стандарта (далее – ФГОС) среднего профессионального образования (СПО) (СПО) по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем от 9 декабря 2016 г. № 1553 для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: колледж федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет» (Колледж ДГУ)

Разработчики:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики и экокомплекса факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Рабочая программа дисциплины одобрена на заседании кафедры специальных дисциплин Колледжа ДГУ

протокол № 7 от «27» сд 2021г.

Зав. кафедрой  /Магомедова А.М./

Рабочая программа дисциплины согласована с учебно-методическим управлением «И» 03 2021г.

Начальник УМУ, д.б.н., проф.  Гасангаджиева А.Г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ДИСЦИПЛИНЫ**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Корпоративная защита внутренних угроз информационной безопасности

1.1. Область применения программы

Рабочая программа дисциплины «Корпоративная защита от внутренних угроз информационной безопасности» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05.Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Корпоративная защита внутренних угроз информационной безопасности» относится к профессиональному модулю «Защита информации в автоматизированных системах программами и программно-аппаратными средствами» профессионального цикла ПССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

Целью изучения дисциплины «Корпоративная защита от внутренних угроз информационной безопасности» является формирование у студентов практических навыков в применении современных корпоративных информационных систем в решении задач, связанных с автоматизацией управленческих, финансовых, экономических и бухгалтерских аспектов деятельности предприятия. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в корпоративных системах.

Задачами изучения дисциплины являются:

- формирование общих представлений о неправомерных действиях сотрудников, приводящих к потере конфиденциальных данных;
- описать общие принципы технологий, применяемых для достижения корпоративной защиты от внутренних угроз информационной безопасности;
- привить умения применять правила обеспечения защиты конфиденциальных данных организации от неправомерных утечек информации;

- освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;
- овладение умением осуществлять сборку, установку, тестирование, использование и обслуживание специализированных программно-аппаратных комплексов по перехвату и анализу трафика данных, циркулирующих в организации (DLP-систем);
- развитие навыков разработки политики информационной безопасности, классификации объектов защиты, понимания аспектов применения нормативно-правовой базы для классификации и расследования инцидентов

Освоение содержания учебной дисциплины «Корпоративная защита внутренних угроз информационной безопасности» обеспечивает достижение студентами следующих результатов:

Общие компетенции

- ОК 01.** Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
- ОК 02.** Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
- ОК 03.** Планировать и реализовывать собственное профессиональное и личностное развитие.
- ОК 04.** Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

Профессиональные компетенции

- ПК 2.1.** Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
- ПК 2.2.** Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
- ПК 2.6.** Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения дисциплины обучающийся должен **уметь:**

- ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;
- анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;
- применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.

В результате освоения дисциплины обучающийся должен **знать:**

- объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;

- понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;
- базовые составляющие в области развития систем информационной безопасности;
- классификацию объектов защиты.

При реализации содержания учебной дисциплины «Корпоративная защита внутренних угроз информационной безопасности» в пределах освоения ОПОП СПО на базе основного общего образования с получением среднего общего образования учебная нагрузка студентов составляет 69 часов, из них аудиторная (обязательная) учебная нагрузка, включая лекции и практические занятия 48 часов; внеаудиторная самостоятельная работа студентов 21 час.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	<i>Объем часов</i>
Максимальная учебная нагрузка (всего)	69
Обязательная аудиторная учебная нагрузка (всего)	
в том числе:	
теоретическое обучение	12
лабораторные работы	
практические занятия (в т.ч. практическая подготовка)	36
контрольные работы	
курсовой проект	
консультация	
Самостоятельная работа обучающегося (всего)	21
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	
<i>Промежуточная аттестация в форме дифференцированного зачета</i>	

2.2. Тематический план и содержание дисциплины «Корпоративная защита внутренних угроз информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) (если предусмотрены)	Объем часов
1	2	3
Раздел 1. Основные понятия и характеристика шифров		
Тема 1.1.	Содержание учебного материала	12
Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке. Установка и настройка агентского мониторинга. Проведена синхронизация с LDAPсервером, раздел персоны заполнен корректно. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность.	2
	Практические занятия/ Лабораторные занятия	6
	<ol style="list-style-type: none"> 1. Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п. 2. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке. 3. Установка и настройка агентского мониторинга. 4. Проведена синхронизация с LDAPсервером, раздел персоны заполнен корректно. 5. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность. 	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	4
Тема 1.2.	Содержание учебного материала	12

Исследование (аудит) организации с целью защиты от внутренних угроз	Угрозы информационной безопасности. Изучение структуры организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. Определить объекты защиты . Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа .	2
	Практические занятия/ Лабораторные занятия	6
	<ol style="list-style-type: none"> 1. Угрозы информационной безопасности. 2. Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. 3. Определить объекты защиты. Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа . 4. Определить каналы передачи данных и потенциальных утечек. Типы циркулирующих данных определены верно. 5. Выявить потоки передачи данных и возможные каналы утечки информации. Заполнить шаблон модели угроз . 6. Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п. Определить перечень нормативных актов РФ, задействованных в рамках модели угроз. 7. Разработать перечень, описание и шаблоны нормативно -правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности. 	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	4
Тема 1.3. Разработка политик безопасности в системе	Содержание учебного материала	12
	Политика безопасности. Модифицировать политики безопасности в системе IWTM в соответствии с получаемыми на практике данными перехвата. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности,	2

корпоративной защиты информации от внутренних угроз	создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации	
	Практические занятия/ Лабораторные занятия	6
	1. Политика безопасности 2. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания. 3. Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п. 4. Модифицировать политики безопасности в системе IWTM в соответствии с получаемыми на практике данными перехвата. 5. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. 6. Работа с интерфейсом управления системы корпоративной защиты информации	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	4
Тема 1.4. Технологии анализа и защиты сетевого трафика	Содержание учебного материала	12
	Технологии анализа и защиты сетевого трафика. Развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной. Межсетевое взаимодействие и туннелированные. VPN. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий	2
	Практические занятия/ Лабораторные занятия:	6
	1. Технологии анализа и защиты сетевого трафика. 2. Развёртывание, настройка и проверка работоспособности VPN -сети на	

	<p>существующей и вычислительной инфраструктуре.</p> <p>3. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной</p> <p>4. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи.</p> <p>5. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN.</p> <p>6. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий</p>	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	4
Тема 1.5. Технологии агентского мониторинга	Содержание учебного материала	11
	Технологии агентского мониторинга. Продемонстрировать знание механизмов работы агентского мониторинга. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами. Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата	2
	Практические занятия/ Лабораторные занятия:	
	<p>1. Технологии агентского мониторинга.</p> <p>2. Продемонстрировать знание механизмов работы агентского мониторинга.</p> <p>3. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами .</p> <p>4. Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата</p>	6
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	3
Тема 1.6. Анализ выявленных	Содержание учебного материала	10
	Анализ выявленных инцидентов. Подготовка отчётов о нарушениях. Применение	2

инцидентов	<p>механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса . Разработка план по дальнейшему расследованию.</p> <p>Текущий контроль (устный опрос) 11 выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.</p>	
	Практические занятия/ Лабораторные занятия:	6
	<ol style="list-style-type: none"> 1. Анализ выявленных инцидентов. 2. Подготовка отчётов о нарушениях. 3. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. 4. Проведение классификацию уровня угроз инцидентов. 5. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса. 6. Разработка план по дальнейшему расследованию. 7. Текущий контроль (устный опрос) 11 выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу. 	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	2
Примерная тематика курсовой работы (проекта) <i>(если предусмотрены)</i>		<i>не предусмотрено</i>
Самостоятельная работа обучающихся над курсовой работой (проектом) <i>(если предусмотрены)</i>		<i>не предусмотрено</i>
	Всего:	69

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Практические занятия проводятся в кабинете интернет-технологий и информатики, оборудованным ПЭВМ с установленным программным обеспечением:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- система программирования «Microsoft Visual Studio Express»;
- программа просмотра pdf-документов Sumatra PDF Reader.

Для самостоятельной работы студентов используется кабинет интернет-технологий и информатики.

Оснащение кабинета:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
- ОС Microsoft Windows
- Антивирус Касперского
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Нестеров, С. А. Информационная безопасность: учебник и практикум для среднего профессионального образования / С. А. Нестеров. - Москва: Издательство Юрайт, 2018. - 321 с. - (Профессиональное образование). - ISBN 978-5-534-07979-1. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/424066>.
2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2020. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/467356> .
3. Моргунов А.В. Информационная безопасность: учебно-методическое пособие Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с.: ил., табл. - 978-5- 7782-3918-0 <https://biblioclub.ru/index.php?page=book&id=576726>
4. Скляр В. В. Обеспечение безопасности АСУТП в соответствии с современными стандартами Москва, Вологда: Инфра-Инженерия, 2018. - 385 с. - 978-5-9729-0230-9 <http://biblioclub.ru/index.php>

Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — URL : <https://urait.ru/bcode/490277>
2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — URL : <https://urait.ru/bcode/468273>
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — URL : <https://urait.ru/bcode/490019>
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru 3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
5. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru 5. ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения

безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: <http://www.aldebarans.ru/komp>, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: <http://ru.wikipedia.org>, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: <http://www.mon.gov.ru>, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: <http://www.pedagogy.ru>, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: <http://www.pntdoc.ru>, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: <http://www.edu.ru>, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: <http://www.tehlit.ru>, свободный. – Загл. с экрана

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
В результате освоения дисциплины обучающийся должен уметь : – правильно эксплуатировать системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации; – использовать методы и средства защиты данных; – планировать организационные мероприятия, проводимые при	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов

<p>криптографической защите информации;</p> <ul style="list-style-type: none"> – устанавливать и настраивать средства защиты информации; – администрировать системы защиты информации; – создавать и модифицировать защищенные сети по заданным схемам; – организовывать межсетевое взаимодействие; – организовывать взаимодействия всех объектов VPN между собой и функционирования туннеля; – обеспечивать работу сервера защищенных соединений. 	<p>выполнения индивидуальных практических работ по решению ситуационных задач.</p>
<p>В результате освоения дисциплины обучающийся должен знать:</p> <ul style="list-style-type: none"> - современные профессиональные технологии в предметной (профессиональной) сфере деятельности; - общие положения об информационной безопасности для телекоммуникационных систем; - организационно-технические и правовые основы использования электронного документооборота в информационных системах; - структура виртуальной защищенной сети; - назначение виртуальной; - технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; - основные компоненты системы защиты информации; - состав программного комплекса ViPNet (Administrator, Client, Coordinator); - основные функции и возможности комплекса ViPNet; - прикладные системы комплекса ViPNet; - ключевую структуру сети ViPNet (ключевая система, формирование и управление ключевой системой); - ЦУС и УКЦ: функции и условия их взаимодействия; 	<p>Интерпретация результатов устного опроса; текущий контроль в форме тестирования; текущий контроль усвоения материала в форме комбинированного опроса; экспертная оценка результатов выполнения домашнего задания; текущий контроль в форме комбинированного опроса; экспертная оценка результатов выполнения домашнего задания.</p>