*Приложение 2.30*

*к ООП по* *специальности*

*10.02.05 Обеспечение информационной безопасности*

*автоматизированных систем*

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

"МЕЖДУНАРОДНЫЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННЫХ СИСТЕМ"

Утверждена

приказом директора

АНО ПО "МКИТИС"

№ от

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.9 КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Химки, 2023

РАССМОТРЕНО

…………………….. Протокол №

« » 20 г.

/ /

СОГЛАСОВАНО

……………………….

« » 20 г.

/ /

Рабочая программа учебной дисциплины ОП.09 «Корпоративная защита от внутренних угроз информационной безопасности» разработана на основе основной образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

# **Организация-разработчик: АНО ПО "МКИТИС"**

СОДЕРЖАНИЕ

|  |
| --- |
| 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ |
| 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ |
| 3.  УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ |
| 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ |

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**1.1. Место дисциплины в структуре основной профессиональной образовательной программы**

Учебная дисциплина «Корпоративная защита от внутренних угроз информационной безопасности» принадлежит к общепрофессиональному циклу.

**1.2****. Цель и планируемые результаты освоения дисциплины:**

|  |  |  |
| --- | --- | --- |
| Код  ПК, ОК | Умения | Знания |
| ОК 01,  ОК 02, ОК 04,  ОК 05, ОК 09, ОК 10;  ПК 1.1, ПК 1.2 | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;  -проводить настройку систем защиты от внутренних угроз информационной безопасности | - способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -возможных угроз безопасности информации в ИТКС;  -способов защиты информации от НСД и специальных воздействий на нее;  -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;  -возможных угроз безопасности информации в ИТКС;  - способов защиты информации НСД и специальных воздействий на нее;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации  -программные и программно-аппаратные средства защиты информации в ИТКС российского производства; |

|  |  |
| --- | --- |
| **Личностные результаты** | **Код личностных результатов** |
| Осознающий себя гражданином и защитником великой страны. | **ЛР 1** |
| Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций. | **ЛР 2** |
| Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих. | **ЛР 3** |
| Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа». | **ЛР 4** |
| Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях. | **ЛР 6** |
| Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности. | **ЛР 7** |
| Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях. | **ЛР 9** |
| Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой. | **ЛР 10** |
| Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры. | **ЛР 11** |
| Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания. | **ЛР 12** |
| **Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности** | |
| Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации. | **ЛР 13** |
| Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм. | **ЛР 14** |
| Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности. | **ЛР 15** |
| **Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации (Московской областью)** | |
| Эффективно демонстрирующий профессиональные навыки в области профессиональной деятельности с учетом специфики рынка труда Московской области. | **ЛР 16** |
| **Личностные результаты реализации программы воспитания, определенные ключевыми работодателями** | |
| Умеющий выстраивать конструктивные взаимоотношения в командной работе по решению общих задач, в том числе с использованием современных средств сетевых коммуникаций. | **ЛР 17** |
| **Личностные результаты реализации программы воспитания, определенные субъектами образовательного процесса** | |
| Сформировано мировоззрение, соответствующее современному уровню развития науки и общественной практики, основанное на диалоге культур, а также различных форм общественного сознания, осознание своего места в поликультурном мире. | **ЛР 18** |

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**2.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной деятельности** | **Объем часов** |
| **Объем образовательной программы** | 46 |
| **Объем работы обучающихся во взаимодействии с преподавателем** | 36 |
| в том числе: | |
| - теоретическое обучение | 20 |
| - лабораторные работы | - |
| - практические занятия | 16 |
| - самостоятельная работа | 10 |
| - промежуточная аттестация (дифференцированный зачет) | - |

**2.2. Тематические план и содержание учебной дисциплины**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала и формы организации деятельности обучающихся** | | | **Объем в часах** | **Осваиваемые элементы компетенций** |
| 7 семестр | | | | | |
| Раздел 1. | Linux в DLP | | | 24 |  |
| Тема 1.1  Изучение серверных и десктопных версий  ОС Linux | Содержание | | | 12 | ОК 1, ОК2, ПК 1.1., ЛР17, ЛР18 |
| Введение в Linux. | | | 2 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Дистрибутивы в Linux. | | | 2 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Man-страницы в Linux. | | | 2 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| GRUB: универсальный загрузчик в Linux. | | | 2 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Процесс загрузки FreeBSD в Linux. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Демоны управления системой в Linux. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Управление процессами в Linux. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Дисковая память в Linux. Драйверы и ядро в Linux | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Практические занятия | | | 12 |
|  | Обзор VirtualBox. | |  |  |
|  | Установка виртуальной машины (Debian 11 desktop). | |
|  | Базовые команды в Linux. | |
|  | Разграничений прав доступа в Linux. | |
|  | Текстовые редакторы Vim, Nano в Linux. | |
|  | Инструменты для работы с текстом в Linux. | |
|  | Файловые подсистемы в Linux. | |
|  | Мониторинг процессов в Linux. | |
|  | Обеспечение целостности и доступности данных. Raid, LVM в Linux. | |
|  | Восстановление данных в Linux. | |
|  | Шифрование данных в Linux. | |
|  | Криптографическая библиотека OpenSSL. | |
| Раздел 2. | Windows Server в DLP | | | 12 |  |
| Тема 2.1  Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP). | Содержание | | | 8 | ОК 1, ОК2, ПК 1.2., ЛР17, ЛР18 |
| Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Технологии агентского мониторинга | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Политики агентского мониторинга, особенности их настройки. Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий;  Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Разработка политик безопасности, анализ выявленных инцидентов | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Разработка и тестирование политик в системе DLP IWTM. Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами; | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Мониторинг трафика. Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером. | | | 1 |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | |  |
| Практические занятия | | | 4 |
|  | | Установка виртуальной машины (Windows Server 2022). |  |
|  | | Обзор Windows Admin Center. |
|  | | Развертывание роли DNS в Windows Server. |
|  | | Развертывание роли DHCP в Windows Server. |
|  | | Развертывание основного контролера домена Active Directory в Windows Server. |
|  | | Развертывание дополнительного контроллера домена в существующий домен Active Directory в Windows Server. |
|  | | Обзор управлений пользовательскими и служебными учетными записями в Windows Server. |
|  | | Обзор введения пользователя в домен. |
|  | | Развертывание инфраструктуры групповых политик в Windows Server. |
|  | | Развертывание роли FTP в Windows Server. |
|  | | Развертывание роли Web Server IIS в Windows Server. |
|  | | Развертывание роли Remote Desktop Services в Windows Server. |
| Самостоятельная работа | | | 10 |
| Чтение и разбор литературы по DLP | | |
| Всего: | | | | 46 |  |

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3.1. Реализация программы дисциплины требует наличия лабораторий корпоративной** **защиты от внутренних угроз информационной безопасности.**

Оборудование лаборатории:

- Стол учительский -1 шт.

- Стул учительский - 1 шт.

- Кресло 16 шт.

- Стул -16 шт.

- Стол компьютерный -16 шт.

- Доска маркерная -1 шт.

- Плакат 5 шт.

- Стенд 1 шт.

Технические средства обучения:

- персональные компьютеры (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память DDR4 объемом не менее 32 Гб; HD 1000 Gb SDD 500ГБ, видеокарта, БП 650 Ватт), объединенные в учебную локально- вычислительную сеть с выходом в сеть Интернет, по количеству обучающихся с лицензионным программным обеспечением: ОС Windows 10, OC Astra Linux/RedOS;

- DLP система InfoWatch;

- монитор с возможностью поворота экрана не менее 90 градусов, не менее 23,8 дюйма, HDMI, USB;

- криптошлюз ПАК ViPNet Coordinator HW100 и учебный комплект VipNet ;

- коммутатор L2 уровень, 16 портов Ethernet стандарта 1000BASE-T;

- маршрутизатор 4 порта Ethernet стандарта 1000BASE-T;

- АПМДЗ Соболь PCI-E.

- Проектор BenQ – 1 шт.

**3.2. Информационное обеспечение обучения**

**3.2.1. Основные печатные источники**

1. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов,. – Спб.: Питер, 2021. – 1008 с. 1 экз

2. Яворски П. "Ловушка для багов"ISBN 978-5-4461-1708-6 Автор Яворски П. 2020 информационные технологии 272 с.

3. Бирюков А А Б59 Информационная безонасность: защита и нанадение. -М.: ДМК Пресс, 2020. - 474 с.: ил

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2020.-272с.:ил.

5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2020.-528с.- (Профессиональное образование)

6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2020. – 616с:ил.

7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2020. – 192с.

8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2020. – 363 с.

9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2020. – 178 с.: ил..

**Интернет ресурсы:**

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2020).

2. Сайт ФСТЭК РФ [Электронный ресурс] – режим доступа: http://www.fstec.ru

3. [Электронный ресурс] – режим доступа: http://www.ancad.ru сайт компании АНКАД

4. [Электронный ресурс] – режим доступа: https://www.cryptopro.ru/ сайт компании КриптоПро

5. ОАО «ИнфоТеКС» [Электронный ресурс] – режим доступа: https://infotecs.ru/ сайт

6. Центр оказания образовательных услуг и подготовки специалистов в области информационной безопасности и эксплуатации средств защиты информации ViPNet. [Электронный ресурс] – режим доступа: https://edu.infotecs.ru/learning/ (2020)

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

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

|  |  |  |
| --- | --- | --- |
| Результаты обучения | Критерии оценки | Методы оценки |
| Умения**:** | | |
| - выявлять и оценивать угрозы безопасности информации в ИТКС; | «Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.  «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.  «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.  «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки. | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24.  Выполнение индивидуальных заданий различной сложности |
| - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24. |
| -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24. |
| -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24.  Выполнение индивидуальных заданий различной сложности |
| -выявлять и оценивать угрозы безопасности информации в ИТКС; | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24. |
| -выявлять и оценивать  техническое  -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; | Наблюдение за выполнением практических заданий № 1, 3-24.  Оценка выполнения практических заданий № 1, 3-24. |
| Знания**:** |  |
| - способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; | Оценка отчетов по выполнению практических работ № 1-2 |
| -типовых программных и программно-аппаратных средств защиты информации в ИТКС; | Опрос по теме 2.1 |
| -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; | Оценка отчетов по выполнению практических работ № 3-24  Экзамен |
| -возможных угроз безопасности информации в ИТКС; | Оценка отчетов по выполнению практических работ № 23-24 |
| -способов защиты информации от НСД и специальных воздействий на нее; | Оценка отчетов по выполнению практических работ № 27-38 |
| -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Опрос по теме 2.15 |
| - способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; | Оценка отчетов по выполнению практических работ № 3-38  Экзамен |
| -типовых программных и программно-аппаратных средств защиты информации в ИТКС; | Оценка отчетов по выполнению практических работ № 3-38  Экзамен |
| -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; | Опрос по темам 3.1-3.2 |

Приложение 1

Обязательное

**КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Личностные результаты** | **Содержание урока (тема, тип урока, воспитательные задачи)** | **Способ организации деятельности** | **Продукт деятельности** | **Оценка процесса формирования ЛР** |
| ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих    ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты  ЛР 18 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты | **Тема:** Проблемы информационной безопасности (12 ч.)  **Тип урока:** обобщения и систематизации знаний и способов деятельности.  Концерт  **Воспитательная задача:**  - формирование уважения к своей будущей профессии  - формирование культуры потребления информации, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве  - формирование представления о возможности карьерного роста при условии непрерывного образования | Подготовка ситуационных сценок о работе специалиста ИБ.  Подготовка проектов безопасности от каждой группы и презентация ее на концерте. | День Информационной безопасности  Концерт, посвященный «Дню ИБ».  Эмоционально окрашенное выступление.  Навык работы на аудиторию и представления себя, как специалиста ИБ | - эмоциональное отношение к своей будущей профессии  - уровень мотивации проявления стремления работать по своей специальности  - навыки анализа и интерпретации информации из различных источников  - демонстрация личностного интереса к профессиональному росту |