***Приложение II.1***

***к программе СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»***

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОП.4 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**2022**

**Составитель:**

**Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ**

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| 1. Паспорт программы учебной дисциплины 2. Структура и содержание учебной дисциплины 3. Условия реализации программы учебной дисциплины 4. Контроль и оценка результатов освоения учебной дисциплины   Приложение 1 |  |

**1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

|  |
| --- |
| Основы информационной безопасности |

*наименование дисциплины*

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

Учебная дисциплина «Основы информационной безопасности» принадлежит к общепрофессиональному циклу.

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

|  |  |  |
| --- | --- | --- |
| Код  ПК, ОК, ЛР | Умения | Знания |
| ОК 01-ОК 02, ОК 04-ОК 05, ОК 09 –ОК 10;  ОК 11;  ОК 12; ПК 2.3, ПК 2.4-ПК 3.1, ЛР 3-4 | Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;  Применять основные правила и документы системы сертификации Российской Федерации;  Классифицировать основные угрозы безопасности информации;  *Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.* | Сущность и понятие информационной безопасности, характеристику ее составляющих;  Место информационной безопасности в системе национальной безопасности страны;  Источники угроз информационной безопасности и меры по их предотвращению;  Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;  Современные средства и способы обеспечения информационной безопасности.  *Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей.* |

**1.3. Рекомендуемое количество часов на освоение программы дисциплины**

Объем работы обучающихся во взаимодействии с преподавателем 36 часов, в том числе:

- 2 часа самостоятельной работы.

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

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

|  |  |
| --- | --- |
| **Вид учебной деятельности** | **Объем часов** |
| **Объем образовательной программы** | 36 |
| **Объем работы обучающихся во взаимодействии с преподавателем** | 32 |
| в том числе: | |
| - теоретическое обучение | 24 |
| - лабораторные работы (если предусмотрено) | - |
| - практические занятия (если предусмотрено) | 8 |
| - курсовая работа (проект) (если предусмотрено) | - |
| - самостоятельная работа[[1]](#footnote-1) | 2 |
| - промежуточная аттестация (дифференцированный зачет) | 2 |

**2.2. Тематические план и содержание учебной дисциплины «Основы информационной безопасности»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала и формы организации деятельности обучающихся** | | | **Объем в часах** | **Коды компетенций, формированию которых способствует элемент программы** |
| **3 семестр** | | | | | |
| **Раздел 1.** | **Информационная безопасность. Основные положения, понятия, определения** | | | **6** |  |
| **Тема 1.1.**  **Актуальность информационной безопасности в системе национальной безопасности России** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Национальные интересы в информационной сфере.  Влияние процессов информатизации общества на составляющие национальной безопасности | | |  |
| Домашнее задание: Чтение и анализ литературы [1] стр. 10-14 | | | |
| **Тема 1.2**  **Сущность и понятие информационной безопасности** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.4., ЛР4 |
| Понятие информационной безопасности. Характеристика составляющих информационной безопасности. Источники и содержание угроз в информационной сфере. Состояние информационной безопасности России и основные задачи по ее обеспечению | | |  |
| Домашнее задание: Чтение и анализ литературы [1] стр.27-42 | | | |
| **Тема 1.3 Принципы обеспечения информационной безопасности** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| **Общеметодологические принципы обеспечения информационной безопасности. Концептуальная модель информационной безопасности** | | |  |
| Домашнее задание: Чтение и анализ литературы [2] стр.6-19 | | |  |
| **Раздел 2.** | **Государственная информационная политика** | | | **6** |  |
| **Тема 2.1**  **Основные положения государственной информационной политики РФ** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.4., ЛР4 |
| Основные положения государственной политики обеспечения информационной безопасности РФ. Первоочередные мероприятия по реализации государственной политики обеспечения ИБ РФ. | | |  |
| Домашнее задание: Чтение и анализ литературы [3] стр. 14-25 | | | |
| **Практические занятия** | | | 2 |
| 1 | Изучение информационно-правовых систем на примере СПС «Гарант» | |
| **Самостоятельная работа обучающихся** | | | 2 |
| Изучение темы **«Современные методы обеспечения информационной безопасности»** | | |
| **Раздел 3.** | **Общие методы обеспечения информационной безопасности** | | | **4** |  |
| **Тема 3.1**  **Общие методы обеспечения информационной безопасности** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Правовые методы обеспечения информационной безопасности. Организационно-технические методы обеспечения информационной безопасности. Экономические методы обеспечения информационной безопасности | | |  |
| Домашнее задание: [2] стр.21-30 | | | |
| **Практические занятия** | | 2 | |
| 2 | Изучение методов поиска документов в информационно-правовой системе «Гарант» |
| **Раздел 4.** | **Общие методы обеспечения информационной безопасности** | | | **10** |  |
| **Тема 4.1**  **Основы защиты информации** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.4., ЛР4 |
| Информация, сообщения, информационные процессы как объекты информационной безопасности. Цели и задачи защиты информации. Классификационная схема понятий в области защиты информации. Концептуальные основы защиты информации | | |  |
| Домашнее задание: [2] стр.29-36 | | | |
| **Практические занятия** | | 2 | |
| 3 | Изучение структуры документов в информационно-правовой системе на примере модели угроз ФСТЭК» |
| **Тема 4.2**  **Источники и носители защищаемой информации** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Понятие «информационный ресурс», классы информационных ресурсов.  Источники и носители защищаемой информации. Концептуальные основы защиты информации | | |  |  |
| Домашнее задание: [2] стр.36-38 | | |  |  |
| **Тема 4.3**  **Виды тайн**  **Государственная тайна. Конфиденциальная информация** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.4., ЛР4 |
| Понятие, определение, классификация информации по видам тайны и степеням конфиденциальности. Жизненные циклы конфиденциальной информации. Защита государственной тайны и конфиденциальной информации. Ответственность за нарушения в области государственной тайны и конфиденциальной информации | | |  |
| Домашнее задание: [2] стр.39-40 | | | |
| **Практические занятия** | | 2 | |
| 4 | Изучение методов поиска документов в информационно-правовой системе «Гарант» |
| **Тема 4.4**  **Угрозы безопасности защищаемой информации** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Понятие, классификация угроз безопасности информации. Дестабилизирующие факторы, виды утечки информации. Типы нарушителей | | |  |
| Домашнее задание: [2] стр.41-43 | | | |
| **Раздел 5.** | **Общие методы обеспечения информационной безопасности** | | | **6** |  |
| **Тема 5.1**  **Классификация типовых объектов информатизации** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Анализ существующих методик определения требований к защите информации  Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Классификация типовых объектов информатизации | | |  |
| Домашнее задание: [2] стр.44-48 | | | |
| **Тема 5.2 Системы защиты информации. Методологические подходы к защите информации и принципы ее организации** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Определение, типизация и проектирование систем защиты информации.  Организация работ по защите информации. Управление функционированием систем защиты информации. Сертификация, основные правила и документы системы сертификации РФ. | | |  |
| Домашнее задание: [2] стр.49-50 | | | |
| **Тема 5.3 Обеспечение безопасности автоматизированных систем.** | **Содержание** | | | **2** | ОК 1, ОК2, ПК 2.3., ЛР3 |
| Понятие и определение автоматизированных систем. Угрозы безопасности автоматизированных систем. Обеспечение безопасности автоматизированных систем  Современные средства и способы обеспечения безопасности информационных систем | | |  |
| Домашнее задание: [2] стр.51-53 | | | |
| **Промежуточная аттестация (диф. зачет)** | | | | | **2** |
| **Всего:** | | | | | **36** |

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы дисциплины требует наличия лабораторий корпоративной защиты от внутренних угроз информационной безопасности или кибербезопасности.

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**

Основные 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 шт.

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..

Дополнительные источники:

1 Руководство администратора Криптон-замок

2. Руководство администратора ППКОП «Астра»

3. Руководство администратора КТМ-256

4. Учебное пособие Структурированная кабельная система NIKOMAX»

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 (освоенные умения, усвоенные знания)** | **Критерии оценки** | **Формы и методы контроля и оценки результатов обучения** |
| **Умения:** | | |
| ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей. | «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, 3-5.  Оценка выполнения практических заданий № 1, 3-5.  Выполнение индивидуальных заданий различной сложности  Диф. зачет |
| ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. | Наблюдение за выполнением практических заданий № 2.  Оценка выполнения практических заданий № 2. |
| ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. | Наблюдение за выполнением самостоятельных работ  Оценка выполнения самостоятельных работ |
| **Знания:** |  |
| - сущность и понятие информационной безопасности, характеристику ее составляющих; | Наблюдение за выполнением практических заданий № 1, 3-5.  Оценка выполнения практических заданий № 1, 3-5.  Выполнение индивидуальных заданий различной сложности  Диф. зачет |
| - место информационной безопасности в системе национальной безопасности страны; | Наблюдение за выполнением практических заданий № 2.  Оценка выполнения практических заданий № 2. |
| - источники угроз информационной безопасности и меры по их предотвращению; | Наблюдение за выполнением самостоятельных работ  Оценка выполнения самостоятельных работ |
| - жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; | Наблюдение за выполнением практических заданий № 1, 3-5.  Оценка выполнения практических заданий № 1, 3-5.  Выполнение индивидуальных заданий различной сложности  Диф. зачет |
| - современные средства и способы обеспечения информационной безопасности. | Наблюдение за выполнением практических заданий № 2.  Оценка выполнения практических заданий № 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 14 Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **Тема:** «Понятие информационной безопасности. Характеристика составляющих информационной безопасности. Источники и содержание угроз в информационной сфере. Состояние информационной безопасности России и основные задачи по ее обеспечению» (12 ч.)  **Тип урока:** изучения и первичного закрепления новых знаний и способов деятельности (исследовательская)  **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 | Написание сочинения на тему: «Моя будущая профессия, карьера» | Эмоционально окрашенный текст о своей будущей профессии (специалист по защите информации) | - 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 |
| ЛР 13 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации    ЛР 14 Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **Тема** «Общеметодологические принципы обеспечения информационной безопасности. Концептуальная модель информационной безопасности» (2 ч.)  **Тип урока:**Изучение и первичного закрепление новых знаний и способов деятельности  **Воспитательная задача:**  - знакомство с возможностями реализации социальных ролей в осваиваемой профессии  - формирование мотивации к проявлению деловых качеств личности,  - побуждение студентов соблюдать правила общения | Конференция на тему: ИБ – возможности будущего  Произвольно обучающиеся разбиваются на группы, находят интересные вакансии на hh.ru, определяют требования и знания для них, создают для себя образовательный маршрут по ИБ. Маршрут представляют в любой творческой форме. От выступления каждого зависит выступление команды. Баллы ставят сами обучающиеся друг другу.  Обучающиеся в команде зарабатывают баллы задавая вопросы соперникам.  Рассказ о будущей профессии и моделирование возможностей практических навыков. | Краткий обзор профессии специалиста по информационной безопасности | - умение представить деловые качества  - умение вести диалог с использованием вербальных средств коммуникации  - соблюдение этических норм общения при взаимодействии с  обучающимися |
| 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 14 Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **Тема** «Общеметодологические принципы обеспечения информационной безопасности. Концептуальная модель информационной безопасности» (2 ч.)  **Тип урока:**Проверки и оценки знаний и способов деятельности  **Воспитательная задача:**  - знакомство с возможностями реализации социальных ролей в осваиваемой профессии  - формирование мотивации к проявлению деловых качеств личности,  - побуждение студентов соблюдать правила общения | Урок-турнир: День безопасного интернета. Небольшая вводная лекция  Студенты садятся за компьютеры и на время проходят турнир, получают понимание о будущей профессии, интересуются темой и предметом. | Краткий обзор профессии специалиста по информационной безопасности, понимание будущей профессии | - умение представить деловые качества  - умение вести диалог с использованием вербальных средств коммуникации  - соблюдение этических норм общения при взаимодействии с  обучающимися |

1. Самостоятельная работа в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема учебной дисциплины в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины. [↑](#footnote-ref-1)