Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

КОЛЛЕДЖ КОСМИЧЕСКОГО МАШИНОСТРОЕНИЯ И ТЕХНОЛОГИЙ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

УП.03.01 УЧЕБНАЯ ПРАКТИКА

10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Королев, 2023 г.

Автор: Синицын К.А. Чебышев А.Ю. Рабочая программа учебной практики УП.03.01. – Королев МО: ТУ им. А.А. Леонова, 2023 г.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО), Учебного плана и примерной основной образовательной программой по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена на заседании цикловой комиссии по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем 16 мая 2023 г., протокол № 6.

Рабочая программа учебной дисциплины рекомендована к реализации в учебном процессе на заседании учебно-методического совета 17 мая 2023 г., протокол № 5.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Область применения программы учебной практики

Рабочая программа учебной практики является частью профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Рабочая программа учебной практики направлена на формирование у студентов практических профессиональных умений, приобретение первоначального практического опыта по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное решение.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ЛР 9	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и

Код	Наименование общих компетенций
	т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 20	Готовый соответствовать ожиданиям работодателей: активный, проектно-мыслящий, эффективно взаимодействующий и сотрудничающий с коллективом, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, демонстрирующий профессиональную жизнестойкость.
ЛР 21	Способный генерировать новые идеи для решения задач цифровой экономики, абстрагироваться от стандартных моделей: перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов.
ЛР 22	Способный проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных
ЛР 23	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 24	Принимающий правила внутреннего распорядка обучающихся в части выполнения обязанностей

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику , устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.2. Цели и задачи учебной практики, требования к результатам освоения практики

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики должен:

Иметь практический опыт	установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; применения основных типов технических средств защиты информации; выявления технических каналов утечки информации; участия в мониторинге эффективности технических средств защиты информации; диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
Уметь	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
Знать	порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических

	каналов утечки информации; структуру и условия формирования технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты информации; номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Рекомендуемое количество часов на освоение рабочей программы учебной практики

Рабочая программа рассчитана на прохождение обучающимися учебной практики в объеме 252 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Объем учебной практики и виды учебной работы

Вид учебных занятий, обеспечивающих практико-ориентированную подготовку	**Объем часов**
Всего занятий	**252**
в том числе:	
Вводное занятие	**2**
Виды работ	**240**
Итоговая аттестация	***10***

2.2. Тематический план и содержание учебной практики

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы по практике		Объем часов	Уровень освоения
1	2		3	4
Вводное занятие	**Содержание учебного материала**			
		Вводное занятие. Исследование задания на практику. Инструктажи. Знакомство с местом прохождения практики.	**2**	1
Раздел 1.	**Развёртывание виртуальной сетевой среды на основе Active Directory**		20	
Тема 1.1. Установка виртуальной машины Windows Server.	**Виды работ**			
	1	Подготовка виртуальной машины. Установка Windows Server.	10	3
	2	Настройка сетевой карты Переименование имени компьютера		3
Тема 1.2. Развертывание Active Directory	**Виды работ**			
	1	Запуск установки ролей и компонентов, установка DNS, DHCP, ADDS	10	3
	2	Настройка сервера как первого домена в локальной сети, активация DHCP сервера, установка области ip адресов		3
Раздел 2.	**Установка шлюза в сеть Интернет для локальной сети**		6	
Тема 2.1 Установка виртуальной машины Windows Server	**Виды работ**			
	1	Подготовка виртуальной машины с двумя сетевыми интерфейсами, установка Windows Server, присоединение машины к домену	4	3
	2	Настройка сетевых интерфейсов, переименования компьютера, присоединение машины к домену		3
Тема 2.2 Развёртывание служб маршрутизации и удаленного доступа	**Виды работ**			
	1	Установка роли сервера «Удалённый доступ»	2	3
	2	Настройка служб маршрутизации для общего доступа к Интернету устройств локальной сети		3
Раздел 3.	**Установка машины нарушителя и подготовка сервера DLP-системы**		22	
Тема 3.1 Установка виртуальной машины Windows 10 (11)	**Виды работ**			
	1	Подготовка виртуальной машины, установка Windows 10 , переименование компьютера	4	2
	2	Присоединение машины к домену		2

Тема 3.2 Установка виртуальной машины Windows Server	**Виды работ**			
	1	Подготовка виртуальной машины, установка Windows Server, переименование компьютера, настройка сетевого интерфейса, присоединение сервера к домену	18	2
	2	Установка СУБД (PostgreSQL, Oracle, или MS SQL Server по выбору из системных требований к DLP-системе)		2
Раздел 4.	**Установка DLP-системы**		24	
Тема 4.1 Установка компонентов ОС Windows и .NETframework	**Виды работ**			
	1	Установка библиотек Visual C 2010, 2013, 2017.	4	2
	2	Установка .NETframework		2
Тема 4.2 Установка DLP-системы	**Виды работ**			
	1	Установка серверных компонентов DLP-системы, Начальная подготовка: установка учетной записи администратора, подключение базы данных	20	2
	2	Установка агентов DLP-системы на компьютеры локальной сети методом развертывание		2
Раздел 5.	**Эксплуатация DLP-системы**		30	
Тема 5.1 Разработка и внедрение правил безопасности	**Виды работ**			
	1	Оценка рисков утечки конфиденциальной информации и подготовка	16	2
	2	Установка в DLP-системе правил безопасности		2
Тема 5.2 Проверка срабатывания правил безопасности	**Виды работ**			
	1	С виртуальной машины нарушителя из-под учетной записи создание инцидентов безопасности по установленным правилам безопасности	14	2
	2	Получение отчетов об инцидентах безопасности		2
Раздел 6.	**Установка средств защиты от несанкционированного доступа**		24	
Тема 6.1 Установка средств защиты от несанкционированного доступа.	**Виды работ**			
	1	Изучение документации средств защиты от несанкционированного доступа.	6	2
	2	Изучение документации по установке программного продукта Secret Net Studio		2
Тема 6.2	**Виды работ**			

Установка Secret Net Studio	1	Начальная подготовка: установка Secret Net Studio	18	2
	2	Настройка Secret Net Studio		2
Раздел 7	**Эксплуатация**		80	
Тема 7.1 Права доступа на ресурсы системы. Многофакторная аутентификация	**Виды работ**			
	1	Выдача прав SNS в соответствии с корпоративными ролями/уровнями допуска	10	2
	2	Задание политики сложности паролей. Вход по идентификатору/смарт-карте		2
Тема 7.2 Мандатное разграничение доступа	**Виды работ**			
	1	Контроль доступа в систему. Контроль доступа к файлам и директориям	20	2
	2	Контроль устройств. Контроль печати. Контроль NTFS-потоков		2
Тема 7.3 Настройка дополнительных механизмов защиты	**Виды работ**			
	1	Шифрование контейнеров	4	2
Тема 7.4 Контроль целостности данных. Гарантированное удаление данных	**Виды работ**			
	1	Расчет контрольных сумм от данных и сравнение с эталонным значением. Контроль оперативного уведомления о нарушении целостности информации. Защита от локального администратора. Контроль создания теневых копий при копировании информации на съемные носители, а также отправке документов на печать	18	2
	2	Уничтожение конфиденциальной информации без возможности последующего восстановления специализированными средствами		2
Тема 7.5 Шаблоны политик	**Виды работ**			
	1	Преднастроенные шаблоны политик в соответствие с требованиями регуляторов	12	2
	2	Создание собственных шаблонов с настроенного АРМ, сравнение текущих настроек АРМ с шаблоном		2
Тема 7.6 Генерация отчетов	**Виды работ**			
	1	Отчет по установленному программному обеспечению на компьютере	16	2
	2	Отчет о защищаемых ресурсах, состоянии и настройках защитных компонентов Отчет о всех электронных идентификаторах, зарегистрированных в системе		2
Раздел 8	**Разработка основной документации по инженерно-технической защите информации.**		44	

Тема 8.1	**Виды работ**			
	1	Рассмотрение системы контроля и управления доступом и ее проектирование	22	2
	2	Разработка основной документации по инженерно-технической защите информации		2
Тема 8.2	**Виды работ**			
	1	Реализация защиты от утечки по цепям электропитания и заземления.	22	2
	2	Рассмотрение принципов работы системы пожарно-охранной сигнализации и ее проектирование		2
Итоговая аттестация	Сдача отчета в соответствии с содержанием тематического плана практики и по установленной форме.		10	3
			252	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством;
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

3.1. Для реализации программы учебной практики должны быть предусмотрены следующие специальные помещения:

Реализация профессионального модуля требует наличия учебной мастерской «Анализ защищенности информационных систем от внешних угроз».

Оборудование мастерской:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- мультимедиа проектор (проектор, экран);
- маркерная доска;
- программное обеспечение общего и профессионального назначения.

Оборудование мастерской:

№	Наименование оборудования	Кол-во
1	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.) Клавиатура Logitech без клавиши Power, подключение по USB Компьютерная мышь: Logitech, подключение по USB	20
2	Экран с проектором Panasonic PT-VW360	1
3	Телекоммуникационный шкаф 42U	2
4	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.)	4
5	Маршрутизатор Cisco ISR 4300 Series	10

6	Коммутатор Cisco 2960 plus	20
7	Межсетевой экран ASA 5506-X	10
8	Платформа RouterBoard MikroTik (Маршрутизатор, коммутатор, PoE)	20
9	Комплексный стенд по защите информации	1

Перечень программных средств:

№	Наименование	Количество лицензий
1	MS Windows 10	20
2	MS Office 2013 Pro Plus	20
3	Adobe reader	20
4	7-zip	20
5	Libre Office	20
6	Notepad++	20
7	Sublime Text 3	20
8	Visual Studio 2019	20
9	Visual Studio Code	20
10	WebStorm	20
11	VirtualBox	20
12	Putty	20
13	OpenServer (Ultimate)	20
14	Linux Debian / Linux Centos	20
15	Cisco Packet Tracer	20
16	Autodesk DWG TrueView	20
17	MS SQL Server Express	20
18	SQL Server Management Studio	20
19	MySQL Community Edition	20

3.2. Информационное обеспечение реализации программы

– **Основные источники:**

1. Современные технологии и технические средства информатизации: Учебник / Шишов О.В. - М.:НИЦ ИНФРА-М, 2021. - 462 с.: 60x90 1/16. - (Среднее профессиональное образование ISBN 978-5-16-011776-8 - Режим доступа: https://znanium.com/read?id=367931

2. Технические средства информатизации: Учебное пособие. Гагарина Лариса Геннадьевна; Москва : Издательский Дом "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2019. - 256 с. - ISBN 978-5-8199-0734-4 http://znanium.com/go.php?id=1021128

3. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2021. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8. https://znanium.com/catalog/document?id=364477

4. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Учеб. пособие. 3-е изд., перераб. и доп. / Р. Г. Магауенов. - М.: Горячая линия Телеком, 2021. - 494с.

5. Бурькова Е. В. Физическая защита объектов информатизации: учебное пособие / Оренбургский государственный университет 2020 – 158 с.

Дополнительные источники:

6. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2021. - 396 с.: 60х90 1/16. - ISBN 978-5-16-010325-9 https://znanium.com/read?id=361160

7. Современные технологии и технические средства информатизации: Учебник / Шишов О.В. - М.:НИЦ ИНФРА-М, 2022. - 462 с.: 60х90 1/16. - (Среднее профессиональное образование) ISBN 978-5-16-017112-8 http://znanium.com/catalog/document?id=379974

8. Бондарев П.В. Физическая защита ядерных объектов: Учебное пособие П.В. Бондарев, А.В. Измайлов, А.И. Толстой; Под ред. Н.С. Погожина. – М.: МИФИ, 2008. – 584 с.

9. Звежинский С.С. Проблема выбора периметровых средств обнаружения // БДИ, 2002. - №4 (44). - С. 36-41.

10. Козинный, А. Сейсмические средства обнаружения для охраны территориально распределенных объектов / А. Козинный, А. Косарев, В. Матвеев // БДИ, 2006. № 4. С. 74-77.

11. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения. — М.: СОЛОН-ПРЕСС, 2012. — 220 с

12. Зенов, А. Ю. Концепция организации обработки информации в системах диагностики и распознавания / А. Ю. Зенов, М. П. Берестень // Инженерный вестник Дона: электрон, научн. журн. 2013. №1. [Электронный ресурс]. -URL: http://ivdon.ru/magazine/archive/nly2013/1568

13. Постановление Правительства РФ «Об утверждении требований к антитеррористической защищенности гостиниц и иных средств размещения, оказывающих гостиничные услуги, и формы паспорта безопасности данных объектов» от 14.04.2017 № 447.

14. Периметровая пассивная сейсмическая система охраны объекта https://cyberleninka.ru/article/n/perimetrovaya-passivnaya-seysmicheskaya-sistema-ohrany-obekta/viewer

15. Введенский, Б. С. Оборудование для охраны периметров / Б. С. Введенский-М.: «Мир безопасности», 2002. -112 с.

16. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. - М.: Горячая линия Телеком, 2010. - 272

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ (редакция, действующая с 1 марта 2021 года) «О персональных данных».

– Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (с изменениями на 9 марта 2021 года)

– Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (с изменениями на 9 марта 2021 года)

– Доктрина информационной безопасности Российской Федерации

– Положение «О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам» (извлечения). Утверждено Постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 № 912-51.

– Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации»

– Федеральный закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

– Указ Президента Российской Федерации от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ (с изменениями на 22 декабря 2020 года) «О техническом регулировании».

– Федеральный закон от 4 мая 2011 г. № 99-ФЗ (с изменениями на 31 июля 2020 года) «О лицензировании отдельных видов деятельности».

– Федеральный закон от 30.12. 2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (с изменениями на 9 марта 2021 года) (редакция, действующая с 27 марта 2021 года).

– Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями на 31 августа 2020 года).

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года).

– Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

– Положение о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26.06.1995 № 608.

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

– Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

– Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

– Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

– **Электронные издания (электронные ресурсы):**

– Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
– Федеральный портал «Информационно - коммуникационные технологии в образовании» http://oso.rcsz.ru/info/kompas/edu.htm
– Всероссийский образовательный портал https://edu-ikt.ru/

– www.dedal.ru.
– www.neurophotonica.ru.

3.3. Общие требования к организации образовательного процесса

Практика является обязательным разделом ООП. Она представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся.

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

По окончании учебной практики обучающимся выставляется оценка на основании текущего и итогового контроля их работы в виде дифференцированного зачета.

3.4. Кадровое обеспечение образовательного процесса

Реализация рабочей программы учебной практики должна обеспечиваться педагогическими кадрами, имеющими среднее профессиональное или высшее профессиональное образование, соответствующее профилю преподаваемой дисциплины (модуля). Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла; эти преподаватели и мастера производственного обучения должны проходить стажировку в профильных организациях не реже одного раза в 3 года.

К образовательному процессу могут быть привлечены преподаватели из числа действующих руководителей и работников профильных организаций, предприятий и учреждений.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется преподавателем в процессе проведения лабораторных занятий и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

Результаты обучения (приобретение практического опыта, освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Приобретённый практический опыт: – использования программно-аппаратных средств защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; ***Освоенные умения:*** – - выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации; ***Усвоенные знания:*** – типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения	Дневник по практике; Отчет по практике; Промежуточный контроль (дифференцированный зачет)

информационной безопасности в телекоммуникационных системах; – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации.	

–

ПРИЛОЖЕНИЕ 1

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Колледж космического машиностроения и технологий

ОТЧЕТ

по учебной практике УП.03.01

по профессиональному модулю ПМ.03. _____

_____

Специальность **10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

Обучающейся 3 курса группы БТС формы обучения очной

Петровой Нины Николаевны

Место прохождения практики

_____

(Название организации)

Срок прохождения практики с «08» июня 202* г. по «21» июня 202* г.

Руководители практики

от организации (при наличии): _____ _____ _____

должность подпись ФИО

МП

от колледжа: преподаватель _____ _____

подпись

Итоговая оценка по практике _____

Королев, 20__

ПРИЛОЖЕНИЕ 2

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Колледж космического машиностроения и технологий

.

«УТВЕРЖДАЮ»
Начальник Центра практической подготовки
_____ Ю.А. Князева
«__» _____ 202_ г.

Задание
на учебную практику
ПП.__ _____
по профессиональному модулю ПМ.03. _____

обучающейся специальности_____
группы _____
(ФИО полностью, номер группы)

Приказ о направлении на практику от «__» _____ 202_ г. № _____

Наименование организации_____

Срок прохождения практики с __.__.202_ г. по__.__.202_ г.

Дата выдачи задания: __.__.202_ г.

Руководитель практики: _____ /_____/
подпись

Председатель цикловой комиссии _____ /_____/
подпись

Ознакомлен:._____
Дата подпись ФИО

Содержание задания на практику:
1.
3.
4.
5.

(ТОЛЬКО ЕСЛИ ОБУЧАЮЩИЙСЯ ПРОХОДИТ ПРАКТИКУ НА ПРЕДПРИЯТИИ)

АТТЕСТАЦИОННЫЙ ЛИСТ ПО ПРАКТИКЕ

_____,
ФИО

обучающийся по специальности _____

группа _____, курс _, форма обучения очная, прошел учебную практику по профессиональному модулю_____ в объеме_____часов с _____ по _____ в _____

Виды и качество выполнения работ в период практики

Виды работ, выполненных обучающимся во время практики	Качество выполнения работ		
	высокое	среднее	низкое
Результат практики	**Программа практики выполнена в ПОЛНОМ/НЕПОЛНОМ объеме** Нужное подчеркнуть		

Характеристика учебной и профессиональной деятельности обучающегося во время прохождения практики

(ТОЛЬКО ЕСЛИ ОБУЧАЮЩИЙСЯ ПРОХОДИТ ПРАКТИКУ НА ПРЕДПРИЯТИИ)

Отзыв-характеристика

на обучающегося по специальности

специальность _____

_____

ФИО

Для заполнения отзыва ответьте, пожалуйста, на следующие вопросы. Выбранные ответы отметьте в таблице любым доступным способом.

№ п/п	Вопрос	Варианты ответов		
1	Понимает ли студент-практикант сущность и социальную значимость своей будущей профессии?	да	нет	не в полной мере
2	Проявляет ли студент-практикант к своей профессии устойчивый интерес?	да	нет	особого интереса не проявляет
3	Способен ли студент-практикант организовать собственную деятельность?	да	нет	требуется контроль руководителя (наставника)
4	Выбирает ли студент-практикант типовые методы и способы выполнения профессиональных задач?	да	нет	выбирает с помощью руководителя (наставника)
5	Оценивает ли студент-практикант эффективность и качество решения различных задач?	да	нет	зависит от сложности задач
6	Принимает ли студент-практикант решения в стандартных и нестандартных ситуациях?	да	нет	требуется помощь руководителя (наставника)
7	Можете ли студент-практикант нести ответственность за принятые решения?	да	нет	иногда сомневается в принятом решении
8	Осуществляет ли студент-практикант поиск необходимой информации, необходимой для эффективного выполнения профессиональных задач?	да	нет	нуждается в помощи руководителя (наставника)
9	Может ли студент-практикант применить необходимую информацию для эффективного выполнения профессиональных задач?	да	нет	применяет под наблюдением наставника
10	Повышает ли студент-практикант свое профессиональное и личностное развитие?	да	нет	стабильного интереса к личностному развитию не проявляет
11	Владеет ли студент-практикант информационной культурой	да		нет
12	Может ли анализировать студент-практикант информацию с использованием информационно-коммуникационных технологий?	да	может, но не всегда	может, но под руководством наставника
13	Может ли оценивать студент-практикант	да	может, но	может, но под

	информацию с использованием информационно-коммуникационных технологий?		не всегда	руководством наставника
14	Работал ли успешно студент-практикант в коллективе и в команде?	да	нет	требуются навыки работы в коллективе
15	Как эффективно студент-практикант общался с коллегами, руководством, потребителями?	проявлял интерес настойчиво		нет, интереса не проявлял
16	Берет ли студент-практикант на себя ответственность за работу членов команды (подчиненных) и за результат выполнения заданий?	да	нет	берёт ответственность неохотно
17	Может ли студент-практикант самостоятельно определять задачи профессионального и личностного развития?	да	нет	нуждается в помощи
18	Может ли студент-практикант заниматься самообразованием?	да	нет	особого интереса к самообразованию не проявляет
19	Может ли студент-практикант осознанно планировать повышение квалификации?	да	нет	требуется убеждать в её необходимости
20	Ориентируется ли студент-практикант в условиях частой смены технологий в профессиональной деятельности?	да	нет	требуется помощь со стороны руководителя

Руководитель практики_____
подпись ФИО

М.П. _____ 2021г.

ДНЕВНИК ПРОХОЖДЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Дата	Содержание работ	Отметка о выполнении

Руководитель практики_____
подпись ФИО

М.П. _____ 202_г.