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

Самообследование

образовательной программы среднего профессионального образования

«Обеспечение информационной безопасности телекоммуникационных систем»

2023

I. Общая информация об образовательной программе

1. Общая характеристика образовательной программы

Образовательная программа по специальности среднего профессионального образования 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденного приказом Министерства образования и науки от 9 декабря 2016 № 1551.

Формы получения образования: допускается только в профессиональной образовательной организации или образовательной организации высшего образования.

Объем образовательной программы, реализуемой на базе основного общего образования с одновременным получением среднего общего образования: 5940 часов.

Сроки получения среднего профессионального образования по образовательной программе, реализуемой на базе основного общего образования с одновременным получением среднего общего образования 3 года 10 месяцев.

Образовательная деятельность при реализации учебных предметов, курсов, дисциплин (модулей), практики, иных компонентов образовательной программы, предусмотренных учебным планом, организуется в форме практической подготовки.

Реализация компонентов образовательной программы в форме практической подготовки осуществляется непрерывно либо путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарным учебным графиком и учебным планом.

Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью. Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

2. Присуждаемая квалификация:

- техник по защите информации.

3. Профессиональные стандарты, на основании которых разработана образовательная программа:

- 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 № 536н, регистрационный номер 840;
- 06.032 Специалист по безопасности компьютерных систем и сетей, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 № 533н, регистрационный номер 842;
- 06.033 Специалист по защите информации в автоматизированных системах, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 № 525н, регистрационный номер 843;
- 06.034 Специалист по технической защите информации, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 09 августа 2022 № 474н, регистрационный номер 844.

4. Форма обучения: очная.

5. Год начала реализации образовательной программы – 2017 г., контингент – 360 чел., количество выпусков – 3.

II. Самообследование образовательной программы

2.1. Соответствие сформулированных в образовательной программе планируемых результатов освоения образовательной программы требованиям профессионального (- ых) стандарта (-ов).

Таблица 2.1.1 Наличие и соответствие ПК и/или ДПК профессиональному(-ым) стандарту(- ам)

Профессиональный стандарт 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, 840, 536н; 06.032 Специалист по безопасности компьютерных систем и сетей, 842, 533н; 06.033 Специалист по защите информации в автоматизированных системах, 843, 525н; 06.034 Специалист по технической защите информации, 844, 474н. (наименование стандарта, регистрационный номер, № приказа)		**Образовательная программа:** Обеспечение информационной безопасности телекоммуникационных систем
№ п/п	**Код и наименование ОТФ и ТФ**	**Наименование ПК**
	1	**2**
1.	06.030 A, Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД. A/01.5, Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; A/02.5, Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД; A/03.5, Техническое обслуживание СССЭ, а	ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей. ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей. ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей. ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей. 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

	также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД.	сетей. ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
2.	06.032 А, Обслуживание средств защиты информации в компьютерных системах и сетях. А/01.5, Обслуживание программно-аппаратных средств защиты информации в операционных системах; А/02.5, Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях; А/03.5, Обслуживание средств защиты информации прикладного и системного программного обеспечения.	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. ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
3.	06.033 А, Обслуживание систем защиты информации в автоматизированных системах. А/01.5, Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем; А/02.5, Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем; А/03.5, Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем.	ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения. ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах. ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета. ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе
4.	06.034 А, Проведение работ по установке и техническому обслуживанию средств защиты информации. А/02.5, Проведение работ по установке, настройке, испытаниям и техническому	ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях. ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации

	обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам; А/03.5, Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа.	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.

2.2. Соответствие содержания образовательной программы требованиям профессионального(-ых) стандарта(-ов)

Таблица 2.2.1 Матрица соответствия элементов образовательной программы ПК образовательной программы

Шифр и название компетенции (ПК и/или ДПК)

ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей.
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.
ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.
ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.
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.
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам 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.
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения.
ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах.
ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета.
ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе

Наименование общепрофессиональных дисциплин и дисциплин профиля, программ практик, междисциплинарных курсов профессиональных модулей СПО, всех дисциплин дополнительного профессионального образования	**ПК 1.1.**	**ПК 1.2.**	**ПК 1.3.**	**ПК 1.4**	**ПК 2.1.**	**ПК 2.2.**	**ПК 2.3.**	**ПК 3.1.**	**ПК 3.2.**	**ПК 3.3.**	**ПК 3.4.**	**ПК 4.1.**	**ПК 4.2.**	**ПК 4.3.**	**ПК 4.4**
ЕН.01 *Математика*	+	+	+		+	+	+	+	+	+	+				
ОП.05 *Основы алгоритмизации и программирования*	+			+											
ОП.06 *Экономика и управление*				+											
ОП.07 *Безопасность жизнедеятельности*	+	+	+		+	+	+	+	+	+	+				
ОП.08 *Организационное и правовое обеспечение информационной безопасности*				+	+				+						
МДК.01.01 *Приемо-передающие устройства, линейные сооружения связи и источники электропитания*	+	+	+	+											
МДК.01.02 *Телекоммуникационные системы и сети*	+	+	+	+											
МДК.01.03 *Электрорадиоизмерения и метрология*	+	+	+	+											
УП.01.01 *Учебная практика*	+	+	+	+											
ПП.01.01 *Производственная практика*	+	+	+	+											
МДК.02.01 *Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты*					+	+	+								
МДК.02.02 *Криптографическая защита информации*					+	+	+								
УП.02.01 *Учебная практика*					+	+	+								
ПП.02.01 *Производственная практика*					+	+	+								
МДК.03.01 *Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты*								+	+	+	+				
МДК.03.02 *Физическая защита линий связи информационно-телекоммуникационных систем и сетей*								+	+	+	+				
УП.03.01 *Учебная практика*								+	+	+	+				
ПП.03.01 *Производственная практика*								+	+	+	+				
МДК.04.01 *Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"*												+	+	+	+
УП.04.01 *Учебная практика*												+	+	+	+

Наименование общепрофессиональных дисциплин и дисциплин профиля, программ практик, междисциплинарных курсов профессиональных модулей СПО, всех дисциплин дополнительного профессионального образования	**ПК 1.1.**	**ПК 1.2.**	**ПК 1.3.**	**ПК 1.4**	**ПК 2.1.**	**ПК 2.2.**	**ПК 2.3.**	**ПК 3.1.**	**ПК 3.2.**	**ПК 3.3.**	**ПК 3.4.**	**ПК 4.1.**	**ПК 4.2.**	**ПК 4.3.**	**ПК 4.4**
ПП.04.01 *Производственная практика*												+	+	+	+
ПДП *Производственная практика (ПРЕДДИПЛОМНАЯ)*	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Государственная итоговая аттестация	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Таблица 2.2.2

Сопоставление тематики выпускных квалификационных работ и требований профессионального (-ых) стандарта (-ов)

№ п/п	**Профессиональный стандарт** 06.030 Специалист по защите информации в телекоммуникационных системах и сетях **Код и наименование ОТФ и ТФ** (необходимые знания, умения)	**Перечень тем ВКР**
1	*2*	*3*
1	A Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД. A/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; A/02.5 Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД; A/03.5 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД.	• Внедрение и разработка программных мер защиты информации в телекоммуникационных системах типовой организации • Внедрение СКУД в комплексную защиту логистического предприятия • Защита веб-ресурсов с применением современных средств и методов обеспечения информационной безопасности • Защита информации АСУТП средствами Kaspersky industrial cyber security • Защита информации в переговорной комнате • Защита информации конфиденциального характера от утечки по техническим каналам с целью повышения эффективности информационной безопасности защищаемого помещения в бизнес-центре «Сигма» • Защита информации ограниченного доступа техническими средствами на примере предприятия машиностроительного комплекса • Защита многофункциональной беспилотной авиационной системы от внешних воздействий радиоэлектронных средств • Защита от утечки аудио сигнала в аналоговой телефонной линии • Защита системы управления многофункциональной беспилотной авиационной системы с использованием технических средств защиты информации от внешних и внутренних угроз • Изучение методов защиты данных в облачных телекоммуникационных системах и разработка системы управления технологий облачной безопасности для предприятия • Интеграция СКУД в комплексную систему защиты информации в центре обработки данных • Использование искусственного интеллекта, нано-технологий в обеспечении защиты информации спутниковых систем вещания • Использование программных и аппаратно-программных средств защиты информации при предоставлении ресурсов локальной сети удаленным пользователям • Использование телекоммуникационных технологий при внедрении в комплекс защиты информации предприятия периметральных средств защиты информации • Исследование возможных методов и путей утечки конфиденциальной информации в
	Профессиональный стандарт 06.032 Специалист по безопасности компьютерных систем и сетей **Код и наименование ОТФ и ТФ** (необходимые знания, умения)	
2	A Обслуживание средств защиты информации в компьютерных системах и сетях. A/01.5 Обслуживание программно-аппаратных средств защиты	

	информации в операционных системах; A/02.5 Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях; A/03.5 Обслуживание средств защиты информации прикладного и системного программного обеспечения.	информационном потоке корпоративной среды и разработка мер по их предотвращению при помощи DLP-систем • Комплекс мер направленный на защиту объекта информатизации с помощью модернизации периметровых и объектовых средств обнаружения на производственном предприятие ООО "Полифонт" • Комплексный подход к защите электронного документооборота на коммерческом предприятии • Криптографические средства защиты информации на предприятии • Методы использования активных/пассивных маскирующих помех для защиты радиоканала беспилотных летательных аппаратов • Модернизация комплекса защиты информации учебного заведения путем введения биометрических методов идентификации и аутентификации • Модернизация комплекса системы защиты информации администрации городского округа Лосино-Петровский • Модернизация комплекса системы защиты информации организации путем внедрения системы защиты от внутренних угроз • Модернизация комплекса системы защиты информации предприятия путем внедрения технических средств охранной сигнализации • Модернизация комплекса системы защиты информационной безопасности на примере "ООО Энергии Технологии" • Модернизация многорубежной системы безопасности автотранспортного предприятия посредством внедрения новых телекоммуникационных технологий • Модернизация системы видео наблюдателя и систем контроля управление доступом на производственном предприятии ООО «Полифонт» • Модернизация системы контроля управления доступом в организации общественного питания • Модернизация средств видео наблюдения и охранной сигнализации объектов информатизации в офисе сотовой связи • Модернизация физических средств защиты центра информатизации на примере предприятия «КТРВ» • Модернизация физической защиты технической библиотеки конструкторского бюро на примере предприятия "Конструкторское бюро химического машиностроения им. А. М. Исаева" • Недостатки ограничения использования внешних накопителей при помощи доменных групповых политик и способы их устранения • Обеспечение информационной безопасности каналов управления автоматизированных систем • Обеспечение информационной безопасности на предприятии с помощью антивируса «Kaspersky Endpoint Securit»
	Профессиональный стандарт 06.033 Специалист по защите информации в автоматизированных системах **Код и наименование ОТФ и ТФ** (необходимые знания, умения)	
3	A Обслуживание систем защиты информации в автоматизированных системах. A/01.5 Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем; A/02.5 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем; A/03.5 Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем.	
	Профессиональный стандарт 06.034 Специалист по технической защите информации **Код и наименование ОТФ и ТФ** (необходимые знания, умения)	
4	A Проведение работ по установке и техническому обслуживанию средств защиты информации. A/02.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам;	

	A/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа.	• Построение vpn-соединений между офисами предприятия на основе продукции компании MikroTik • Построение защищённых систем передачи данных мониторинга состояния нефтегазового комплекса • Построение системы защиты информации для отдела на основе программных продуктов InfoWatch • Построение системы удаленного доступа на предприятии с использованием собственного удостоверяющего центра • Практическое использование пентеста для обнаружения возможных уязвимостей и недостатков в сети • Применение DLP-систем как инструмента обеспечения информационной безопасности компании • Применение и роль средств обнаружения при модернизации комплексной системы защиты организации • Применение интегрированных средств видеонаблюдения в комплексных системах безопасности на предприятии • Применение нано-технологий для защиты персональных данных в телекоммуникационных системах • Применение технологии Блокчейн в целях защиты персональных данных в телекоммуникационных системах, медицинского учреждения ГАУЗ МО "Королёвская стоматологическая поликлиника" • Проектирование и внедрение систем защиты предприятия от радиотехнических средств, разведки и подавления • Проектирование комплекса системы защиты информации в кабинете руководителя организации «ООО Звездочка» • Разработка и реализация системы защиты информации в телекоммуникационной сети на основе технологии блокчейн • Разработка комплексной системы защиты информации для типового малого офиса в бизнес центре • Разработка комплексной системы защиты информации объекта информатизации торгового предприятия • Разработка многофакторной системы защиты информации объекта информатизации с использованием биометрических методов идентификации и аутентификации • Разработка мобильного многофункционального аппаратно-программного комплекса выявления уязвимостей в компьютерных локальных и вычислительных сетях • Разработка системы видеонаблюдения в офисном помещении • Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в кабинете руководителя • Разработка системы защиты телекоммуникационных сетей с использованием методов

		машинного обучения для предотвращения кибератак • Роль телекоммуникационных технологий и средств обнаружения в комплексной системе защиты транспортных средств • Система защиты информации ВПК и государственных учреждений от радиолокационных и оптических средств разведки • Система обеспечения безопасного беспроводного доступа к корпоративной вычислительной сети предприятия • Система обеспечения защиты информации в выделенном помещении • Система обеспечения защиты информации в переговорной комнате • Система удаленного доступа работников к сети организации на основе OpenVPN • Системы выявления несанкционированного доступа к ресурсам мобильных операционных систем • Совершенствование комплекса радиоэлектронного подавления и защита информации наземных радиолокационных систем предупреждения о ракетном нападении противоборствующей стороны • Совершенствование комплекса радиоэлектронной защиты РЭС орбитального компонента ракетно-космической системы в ходе радиоэлектронно-информационного конфликта • Совместное использование продукции компании «Код безопасности» и компании «Индид» для усиления комплексной защиты информации предприятия • Способы и методы защиты телекоммуникационных и навигационных систем на МБАС • Средства обнаружения киберугроз и борьбы с ними на примере Kaspersky Scan Engine 2.1 • Стеганографические методы защиты информации на предприятии • Технологии фишинговых атак и противодействия им • Физическая защита линий связи организации с использованием комплексных технических решений

2.3. Соответствие материально-технических, информационно-коммуникационных, учебно-методических ресурсов, непосредственно влияющих на качество профессиональной подготовки выпускников

1) Материально-технические ресурсы

Учебный кабинет «Математика».

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- учебная доска;
- рабочее место преподавателя;
- стационарные стенды;
- справочные пособия;
- медиатека (мультимедиа разработки и презентации к урокам);
- дидактический материал (варианты индивидуальных заданий)
- чертежные инструменты.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- мультимедиа проектор;
- интерактивная доска.

Учебный кабинет «Инженерная графика».

Оборудование учебного кабинета:

- рабочее место обучающихся (по количеству обучающихся);
- рабочее место преподавателя;
- комплект учебно-методической документации;
- учебно-наглядные пособия
- комплект моделей, деталей, натурных образцов, сборочных единиц.

Технические средства обучения:

- компьютеры с программой САПР и лицензионным обучением;
- мультимедийный проектор.

Кабинет социально-экономических дисциплин (экономики и менеджмента) и лаборатории информационных технологий.

Оборудование учебного кабинета:

- персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия, мультимедийное оборудование.
- посадочные места по количеству обучающихся.

Кабинет безопасности жизнедеятельности.

Оборудование кабинета:

- рабочее место преподавателя,
- парты учащихся (в соответствие с численностью учебной группы),
- доска,

- персональный компьютер с лицензионным программным обеспечением,
- мультимедиа проектор и экран.

Учебный кабинет нормативного правового обеспечения информационной безопасности и лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, подключение к сети Интернет, проектор, презентации уроков, стенды, плакаты, методические пособия, справочная правовая система.

Оборудование лаборатории информационных технологий: рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»; программное обеспечение сетевого оборудования; мультимедийное оборудование; программное обеспечение (справочная правовая система).

Учебная мастерская «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,количество

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 42U2

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

2) Кадровые ресурсы

Информация о списочном составе педагогических работников, участвующих в реализации образовательной программы, размещена на сайте Технологического университета.

2.4. Подтвержденное участие работодателей, в том числе представителей крупных организаций, в проектировании и реализации образовательной программы

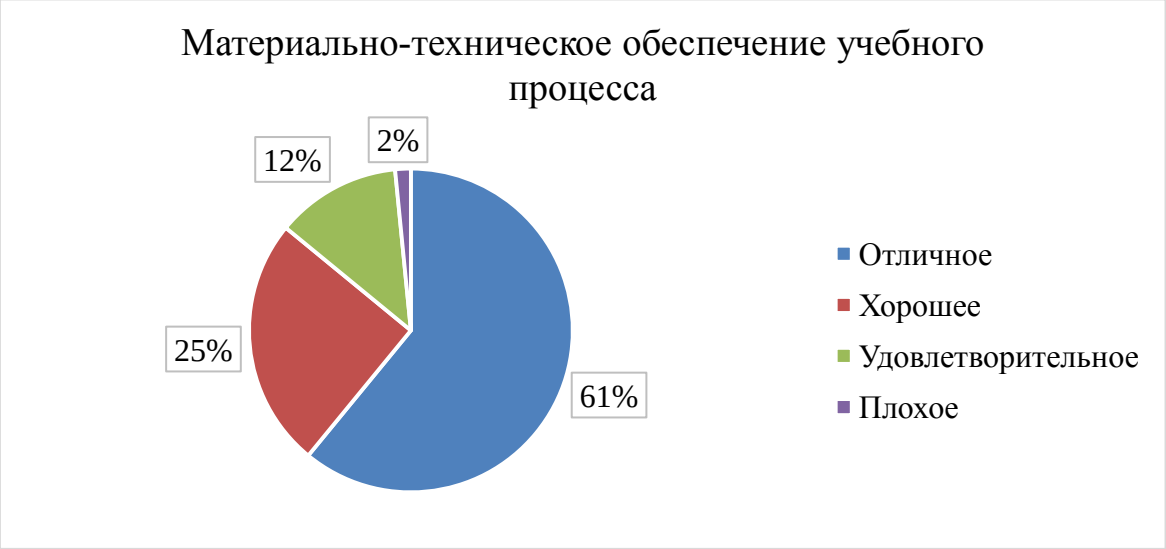
Основная образовательная программа ежегодно рассматривается и согласовывается с представителями работодателей. Работодатели пишут

рецензию на основную образовательную программу. Также составляется акт согласования программ профессиональных модулей, практик, фондов оценочных средств, заданий на производственную практику.

2.5. Результаты опросов студентов, преподавателей и работодателей

Результаты анкетирования обучающихся


Какой формат учебных занятий для вас наиболее комфортен?
6%
22%
72%
Традиционный формат (в аудитории)
В дистанционном формате (лекции, записанные заранее, выкладываются на портале
Онлайн

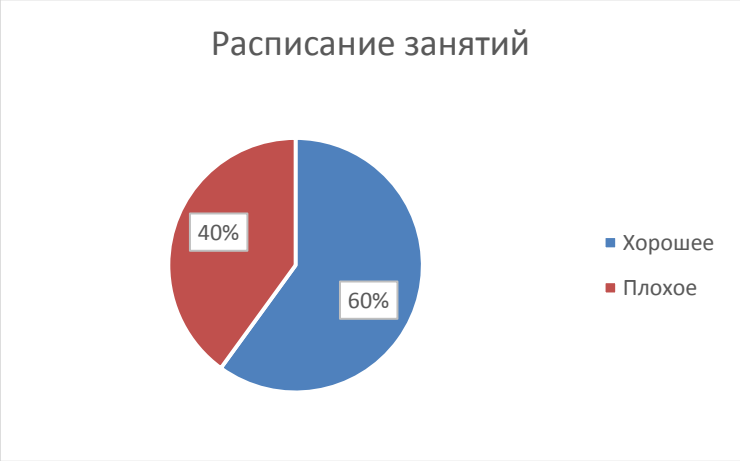

Материально-техническое обеспечение учебного процесса
2%
12%
25%
61%
Отличное
Хорошее
Удовлетворительное
Плохое


Удовлетворены ли Вы возможностями и качеством работы электронной информационной образовательной среды?
0%
2%
28%
70%
Полностью удовлетворен
Скорее удовлетворен
Скорее не удовлетворен
Полностью не удовлетворен

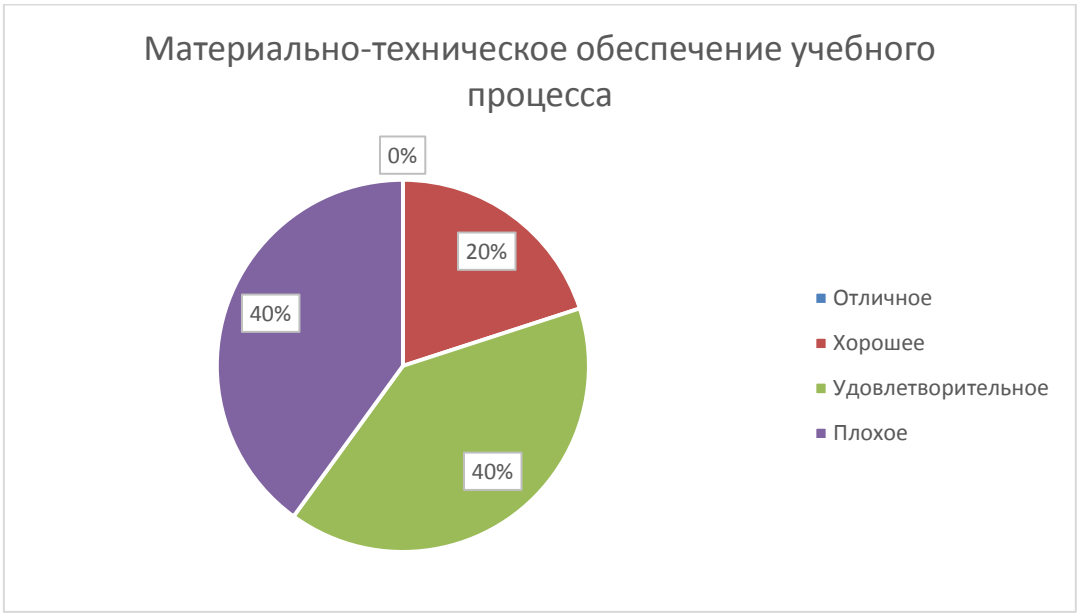

Удовлетворены ли Вы количеством и качеством электронных библиотечных ресурсов и фондом библиотеки?
3%
0%
16%
81%
Полностью удовлетворен
Скорее удовлетворен
Скорее не удовлетворен
Полностью не удовлетворен


Удовлетворены ли Вы психологическим климатом в колледже?
0%
2%
14%
84%
Полностью удовлетворен
Скорее удовлетворен
Скорее не удовлетворен
Полностью не удовлетворен

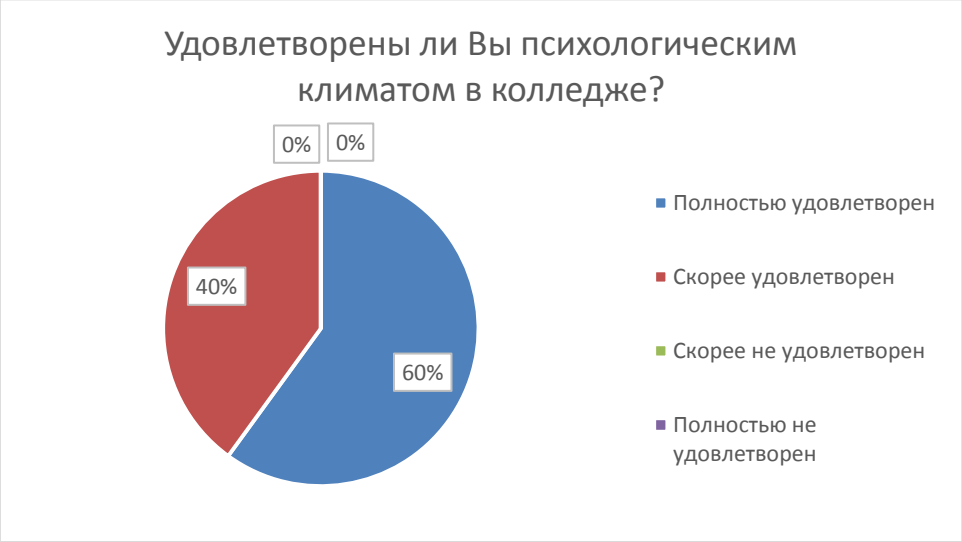
Результаты анкетирования преподавателей



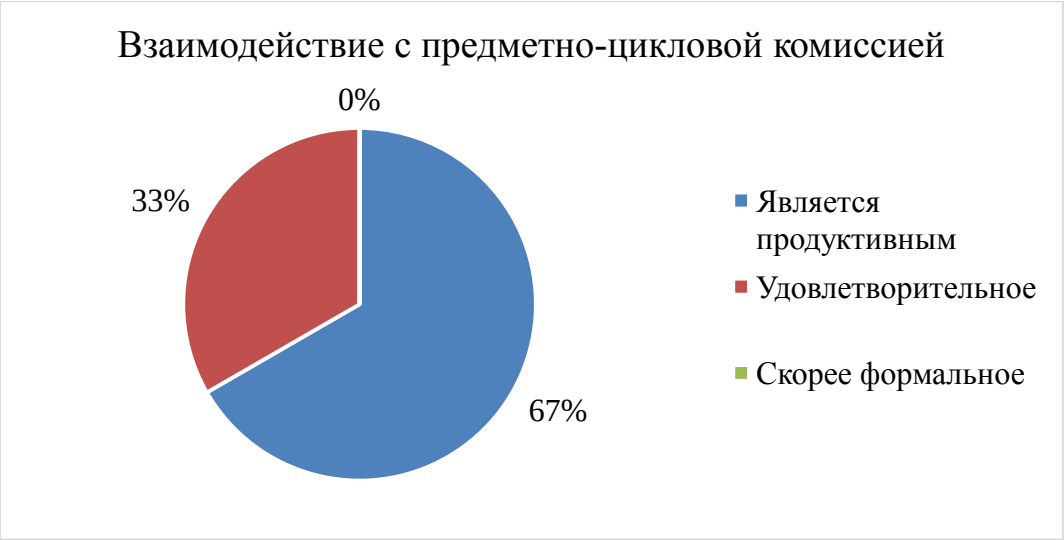

Какой формат учебных занятий для вас наиболее комфортен?
0%
20%
80%
Традиционный формат (в аудитории)
В дистанционном формате (лекции, записанные заранее, выкладываются на портале
Онлайн


Материально-техническое обеспечение учебного процесса
0%
20%
40%
40%
Отличное
Хорошее
Удовлетворительное
Плохое


Удовлетворены ли Вы возможностями и качеством работы электронной информационной образовательной среды?
0%
20%
20%
60%
Полностью удовлетворен
Скорее удовлетворен
Скорее не удовлетворен
Полностью не удовлетворен



Результаты анкетирования работодателей


Взаимодействие с предметно-цикловой комиссией
0%
33%
67%
Является продуктивным
Удовлетворительное
Скорее формальное


Реализуемые образовательные программы, на Ваш взгляд:
0%
100%
Являются актуальными
Требуют небольшой корректировки
Следует полностью переработать


Уровень подготовки по специальным дисциплинам
0%
33%
67%
Высокий
Средний
Низкий


Уровень подготовки по базовым техническим дисциплинам
0%
33%
67%
Высокий
Средний
Низкий


Используете ли Вы возможности электронной информационной образовательной среды?
0%
33%
67%
Использую для просмотра рейтинга студентов
Использую для просмотра рейтинга студентов и образовательных программ
Не использую


Выпускники Колледжа по Вашему мнению:
33%
67%
Полностью готовы к работе на предприятии, дополнительное обучение не требуется
Имеют необходимую базовую подготовку, требуется небольшое обучение с учетом специфики


Удовлетворены ли Вы коммуникационными и организаторскими навыками выпускников?
0%
100%
Полностью удовлетворен
Скорее удовлетворен
Скорее не удовлетворен
Полностью не удовлетворен