Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гнатюк Сергей Иванович
Должность: Первый проректор
Дата подписания: 28.08.2025 14:43:25
Уникальный программный идентификатор:
5ede28fe5b714e680817c5c132d4ba793a6b4432

ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ К.Е. ВОРОШИЛОВА»

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
учебной
(вид практики)

профессионального модуля

**ПМ 02 Защита информации в информационно-телекоммуникационных
системах и сетях с использованием программных и программно-
аппаратных (в том числе, криптографических) средств защиты**

10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем
(код, наименование профессии/специальности)

Рассмотрено и согласовано цикловой комиссией компьютерных дисциплин.

Протокол № 2 от «06» сентября 2023 г.

Разработана на основе ФГОС СПО РФ и ПООП СПО для специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (утверждён приказом Министерства образования и науки от 9 декабря 2016 №1551).

Организация разработчик: Политехнический колледж ЛГАУ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ учебной

УП 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты (указать вид практики)

1.1. Место учебной практики в структуре образовательной программы.

Программа учебной практики является частью основной образовательной программы по специальности (далее – ОПОП) по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

в части освоения вида профессиональной деятельности:

По профессиональному модулю: ПМ. 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

1.2 Цели и задачи учебной практики.

С целью овладения указанными видами деятельности обучающийся в ходе данного вида практики должен:

иметь практический опыт:

- определения необходимых средств криптографической защиты информации;
- использования программно-аппаратных криптографических средств защиты информации;
- установки, настройки специализированного оборудования криптографической защиты информации;
- применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
- шифрования информации.

уметь:

- 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;

знать:

- 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 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;

1.3. Количество часов на учебную практику:

Всего 3 недели 108 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

Результатом _____ учебной _____ практики является освоение общих компетенций (ОК)

Код	Наименование результата обучения
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 развитие
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

профессиональных компетенций (ПК)

Вид профессиональной деятельности	Код	Наименование результатов практики
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	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 систем и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1 Тематический план

Коды профессиональных компетенций	Наименование профессиональных модулей	Объем времени, отведенный на практику (в неделях,	Сроки проведения
ПК 2.1	ПМ. 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	3 недели – 108 часов	
ПК 2.2			
ПК 2.3			

3.2 Содержание практики

Наименование профессионального модуля	Наименование ПК	Виды работ	Объем часов
ПМ. 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	ПК 2.1– ПК 2..3	Тема 1. Администрирование системы антивирусной защиты.	36
		Тема1.1 Инструктаж по технике безопасности. Организация рабочего места. Изучение нормативных документов. Аппаратно-программные средства идентификации и аутентификации.	8
		Тема1.2 Инструктаж по технике безопасности. АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	7
		Тема1.3 Инструктаж по технике безопасности. Настройка локальной политики безопасности Windows. Параметры безопасности	7
		Тема1.4 Инструктаж по технике безопасности. Восстановление информации типовыми средствами Программы восстановления информации	7
		Тема1.5 Инструктаж по технике безопасности. Криптон-шифрование	7
		Тема 2 Подключение, установка драйверов, настройка программных средств шифрования Криптон.	36
		Тема 2.1 Инструктаж по технике безопасности. Применение методов шифрования перестановкой	8
		Тема 2.2 Инструктаж по технике безопасности. Криптоанализ методов замены	7
		Тема 2.3 Инструктаж по технике безопасности. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне.	7

Наименование профессионального модуля	Наименование ПК	Виды работ	Объем часов
		Тема 2.4 Инструктаж по технике безопасности. Защита информации в сетях организованных по технологии беспроводного доступа	7
		Тема 2.5 Инструктаж по технике безопасности. Перспективы развития криптографии.	7
		Тема 3 Составление алгоритма шифра	30
		Тема 3.1 Инструктаж по технике безопасности. Стандарт шифрования данных DES.	8
		Тема 3.2 Инструктаж по технике безопасности. Алгоритм Диффи-Хелмана	8
		Тема 3.3 Инструктаж по технике безопасности. Проблема распределения ключей симметричного шифрования.	7
		Тема 3.4 Инструктаж по технике безопасности. Возведение в степень и логарифмы	7
		Промежуточная аттестация: дифференцированный зачет	6
		Всего:	108

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1 Требования к документации, необходимой для проведения практики:

Учебная практика проводится на основании следующих документов:

- ФГОС СПО специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;
- Основная профессиональная образовательная программа (ОПОП) специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;
- Примерной программы профессионального модуля ПМ. 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты;
- Положение о практической подготовке обучающихся, осваивающих основные профессиональные образовательные программы среднего профессионального образования Политехнического колледжа ЛГАУ;
- Методические рекомендации по проведению учебной и производственной практики специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

4.2 Требования к материально-техническому обеспечению

Реализация программы учебной практики предполагает наличие **лаборатории** Программных и программно-аппаратных средств защиты информации

Лаборатория должна быть оснащена антивирусными программными комплексами; аппаратными средствами аутентификации пользователя; программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации; средствами защиты информации от НСД, блокирования доступа и нарушения целостности; программными средствами криптографической защиты информации; программными средствами выявления уязвимостей и оценки защищенности ИТКС, анализа сетевого трафика;

Оборудование учебного кабинета и рабочих мест кабинета:

- системы разграничения доступа;
- межсетевые экраны;
- средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;
- комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

4.3 Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. 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, 2016. – 363 с.

2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – СПб.: Питер, 2015. – 944 с.

3. Томаси У. Электронные системы связи.- М.: Техносфера, 2016. -1360с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013. – 172 с.

6. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

7. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Издво: ДМК Пресс, - 2012

9. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2009. - 192с.

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с .

Основные электронные источники:

11. Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

12. www.fstec.ru

13. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

14. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

15. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>

16. <http://www.morion.ru/> <http://www.nateks.ru/> <http://www.iskratel.com/>
<http://www.ps-ufa.ru/> <http://3m.com/>

17. <http://www.rusgates.ru/index/php> - Материалы сайта завода «Ферроприбор»

Дополнительные источники:

18. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

19. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

20. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

21. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

22. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

23. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

24. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

25. 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».

26. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

27. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

28. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

29. 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.

30. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

4.4 Требования к руководителям практики от образовательной организации (учреждения) и организации

Требования к квалификации педагогических кадров, осуществляющих руководство учебной практики по специальности должна обеспечиваться педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой учебной практики. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла. Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже одного раза в 5 лет.

4.5 Требования к соблюдению техники безопасности и пожарной безопасности

Учебная практика проводится согласно Инструкции по технике безопасности при проведении соответствующего вида практики.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций обеспечивающих их умений.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и
<p>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.</p>	<ul style="list-style-type: none"> – Знание основных протоколов идентификации и аутентификации в телекоммуникационных системах; – Умение выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; 	<p>Текущий контроль в форме защиты практических работ. Оценка защиты отчета по учебной практике практики тестирование защита практических работ;</p>
<p>ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.</p>	<ul style="list-style-type: none"> – Знание типовых криптографических алгоритмов, применяемые в защищенных телекоммуникационных системах; – Умение пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации; 	<p>Текущий контроль в форме защиты практических работ. Оценка защиты отчета по учебной практике</p>
<p>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.</p>	<ul style="list-style-type: none"> – Знание особенностей применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; – Умение пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации; 	<p>Текущий контроль в форме защиты практических работ. Оценка защиты отчета по учебной практике</p>

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	демонстрация интереса к будущей профессии	интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики; оценка на защите отчета по практике
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Выбор и применение методов и способов решения профессиональных задач. Самоанализ эффективности и качества выполнения профессиональных задач.	интерпретация результатов наблюдений за деятельностью студентов в процессе освоения образовательной программы; мониторинг и оценка эффективной организации профессиональной деятельности
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие	Умение решать стандартных и нестандартных профессиональных задач в области ликвидации инфекционных и инвазионных заболеваний	наблюдение и оценка действий на учебной практике; оценка результатов дифференцированного зачета.
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством.	Взаимодействие с обучающимися, преподавателями и ветеринарными специалистами АПК в ходе обучения; Грамотное взаимодействие с владельцами животных в	использование электронных источников; накопительная оценка за представленную информацию на
ОК 9. Использовать информационные технологии в профессиональной деятельности	Работа с персональным компьютером, Интернетом, другими электронными носителями на уровне пользователя.	отзыв руководителя по практике о деятельности обучающегося на учебной практике
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;	отзыв руководителя по практике о деятельности обучающегося на учебной практике