МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Рабочая программа учебной дисциплины

ОП 09. Защита информационных процессов в компьютерных системах

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2023

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчик:
Рогачева О.Н., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	13

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Защита информационных процессов в компьютерных системах

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место учебной дисциплины в структуре ППССЗ:

Дисциплина является общепрофессиональной и входит в общепрофессиональный цикл.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен **уметь**:

У1 определять виды угроз безопасности информации и информационных процессов;

У2 применять методы защиты информации в компьютерных системах и компьютерных сетях;

У3 применять методы криптографической защиты информации;

У4 классифицировать компьютерные вирусы и использовать антивирусные программы;

У5 проектировать технические средства обеспечения безопасности и применять аппаратно-программные средства защиты информации от НСД;

У6 применять правовые нормы защиты информации и информационных процессов.

У7 ориентироваться в нестандартных условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий.

В результате освоения учебной дисциплины обучающийся должен **знать**:

З1 основные угрозы информации в компьютерных системах;

З2 специфику возникновения угроз в открытых сетях;

З3 основные руководящие документы в области защиты информационных процессов в компьютерных системах;

З4 особенности защиты информации на узлах компьютерной сети;

З5 основные категории требований к программной и программно-аппаратной реализации средств защиты информации;

З6 требования к защите автоматизированных систем от НСД.

Профессиональные (ПК) и общие (ОК) **компетенции**, которые актуализируются при изучении учебной дисциплины:

ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК.06 Проявлять гражданско - патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК.09 Использовать информационные технологии в профессиональной деятельности

ОК.10 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:

знать и понимать:

- понимание принципов работы специалиста по информационной безопасности и их применение;
- знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;
- регламентирующие документы в области безопасности информационных систем;
- регламентирующие документы в области охраны труда и безопасности жизнедеятельности;
- важность организации труда в соответствии с методиками;
- методы и технологии исследования;
- важность управления собственным профессиональным развитием;
- скорость изменения Ит-сферы и области информационной безопасности, а также важность соответствия современному уровню.
- важность умения слушать собеседника как части эффективной коммуникации;
- роли и требования коллег и наиболее эффективные методы коммуникации;
- важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими;
- способы разрешения непонимания и конфликтующих требований;

1) уметь:

- интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;
- применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;
- настраивать сетевые устройства;
- администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;
- установка агентской части системы корпоративной защиты от внутренних угроз;
- запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров;
- настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом;
- уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки;

1.4. Планируемые личностные результаты освоения рабочей программы

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в

сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.5. Количество часов на освоение рабочей программы учебной дисциплины:

максимальной учебной нагрузки обучающегося - 128 часов, в том числе: аудиторной учебной работы обучающегося - 118 часов, из них в форме практической подготовки – 118 часов; в том числе практических занятий - 56 часов; самостоятельной учебной работы обучающегося - 10 часов; консультаций - 0 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**128**
Аудиторная учебная работа (обязательные учебные занятия) (всего)	**118**
из них в форме практической подготовки	**118**
в том числе:	
лекционные занятия	**60**
лабораторные работы	
практические занятия	**56**
контрольные работы	
в том числе:	
Изучение материала по литературным источникам Поиск информации Подготовка сообщения	3 4 3
Промежуточная аттестация: *дифференцированный зачет*	**2**

2.2. Тематический план и содержание учебной дисциплины Защита информационных процессов в компьютерных системах

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся		Объем часов	Коды личностных результатов, формированию которых способствует элемент программы
1	2		3	
Тема 1. Анализ потенциальных угроз безопасности информационных процессов в компьютерных системах	Содержание учебного материала, в том числе в форме практической подготовки		**18/18**	У1-У7 З1-З6 ЛР 4 ЛР 7
	1	Проблемы информационной безопасности. Основные понятия и положения защиты информации в компьютерных сетях (далее КС).	2	
	2	Правовые основы защиты информации информационных процессов в компьютерных системах.	2	
	3	Источники угроз. Случайные и преднамеренные угрозы.	2	
	4	Постановка задачи анализа потенциальных угроз.	4	
	5	Анализ и защита от утечки компьютерной информации по каналам ПЭМИН.	4	
	6	Анализ электромагнитных излучений и наводок в компьютерных системах.	4	
	Лабораторные занятия		*	
	Практические занятия, в том числе в форме практической подготовки Основные угрозы информационной безопасности. Основные принципы формирования режима обеспечения безопасности. Характеристики изучения протоколов обмена. Анализ спектра протоколов обмена. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и при наличии изолированного компьютера.		**10/10** 2 2 2 2 2	
	Контрольные работы		*	
Тема 2. Методы защиты	Содержание учебного материала		**18/18**	У1-У7 З1-З6 Р 4
	1.	Организационные методы защиты информационных процессов в компьютерных системах.	2	

	2.	Ограничение и контроль доступа, идентификация и установление доступа	2	ЛР 7
	3.	Инженерно-технические методы защиты информационных процессов.	4	ЛР 10
	4.	Программно-аппаратные методы защиты информации.	2	ЛР 11
	5.	Программно-аппаратные методы защиты информационных процессов.	2	
	6.	Защита электронных документов.	6	
	Лабораторные занятия			
	Практические занятия, в том числе в форме практической подготовки		**20/20**	
	Ограничение доступа.		2	
	Разграничение доступа.		2	
	Контроль доступа.		2	
	Концепция построения систем разграничения доступа.		2	
	Разграничение доступа к документам, ресурсам ПЭВМ и сети.		2	
	Разграничение доступа к документам, ресурсам ПЭВМ и сети.		2	
	Привязка к особенностям файловой системы.		2	
	Защита документа при его передаче.		2	
	Защита документа при его обработке, хранении и исполнении.		2	
	Защита данных в каналах связи.		2	
	Контрольные работы		*	
Тема 3. Информационные процессы и системы	Содержание учебного материала, в том числе в форме практической подготовки		**12/12**	У1-У7 З1-З6 ЛР 4
	1	Модель ISO/OSI. Физический уровень.	4	
	2	Канальный уровень.	2	
	3	Модель ISO/OSI. Сетевой уровень.	2	
	4	Транспортный уровень	2	
	5	Открытый ключ. Система электронной подписи.	2	
	Лабораторные занятия		*	
	Практические занятия, в том числе в форме практической подготовки		**8/8**	
	Криптографическая защита.		2	
	Шифрование.		2	
	Системы для выработки секретных ключей.		2	
	Алгоритм выработки уникальных секретных ключей.		2	
Тема 4. Особенности защиты информации на узлах	Содержание учебного материала, в том числе в форме практической подготовки		**12/12**	У1-У7 З1-З6 ЛР 4
	1	Администрирование серверных систем и приложений.	4	
	2	Основные виды работ администрирования серверных систем и приложений.	4	

компьютерной сети	3	Резервное копирование. Журнализация изменений. Мультиплексирование и архивирование.	4	ЛР 7 ЛР 10 ЛР 11
	Лабораторные занятия		*	
	Практические занятия, в том числе в форме практической подготовки Основные виды работ администрирования серверных систем и приложений. Настройка и администрирование сервера. Настройка системы безопасности, контроль и отчеты по трафику. Настройка системы безопасности, контроль и отчеты по трафику. Классическое администрирование. Автоматизация управления ПО. Обеспечение информационной безопасности СУБД. Мониторинг сетевых узлов. Мониторинг сетевого трафика.		**18/18** 2 2 2 2 2 2 2 2 2 2	
Самостоятельная работа обучающихся	Изучение материала по литературным источникам: «Предпосылки появления угроз» Поиск информации «Основные непреднамеренные искусственные угрозы» Подготовка сообщения «Основные преднамеренные искусственные угрозы» Изучение материала по литературным источникам: «Страхование как метод защиты информации» Поиск информации «Защита информационных технологий» Изучение материала по литературным источникам: Хэширование и хэш-функции. Поиск информации «Мониторинг сетевого трафика»		**10**	
	Дифференцированный зачет		**2\2**	
	Всего:		**128**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия лаборатории Программного обеспечения и сопровождения компьютерных систем.

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

3.2. Информационное обеспечение обучения:

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб.пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ» : ИНФРА-М, 2020.- 416с.
2. Основы информационной безопасности: учебник/Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А.. – М.: Академия. 2019-256 с.

Дополнительные источники:

3. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
4. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
5. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
6. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
7. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
8. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
9. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту

информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
10. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2013.
11. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.
12. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
13. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д.А.–М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

Электронные издания (электронные ресурсы)

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru –
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru 9. Федеральная служба по техническому и экспортному контролю
7. (ФСТЭК России) www.fstec.ru

Цифровая образовательная среда СПО PROFобразование:

1. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 263 с. — ISBN 978-5-4497-0666-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/97553 (дата обращения: 12.11.2020). — Режим доступа: для авторизир. Пользователей
2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 125 c. — ISBN 978-5-4487-0299-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/77318 (дата обращения: 13.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS

https://www.iprbookshop.ru/89443.html

https://www.iprbookshop.ru/6991.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачета.

Результаты обучения (освоенные умения, усвоенные знания), с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Формы и методы контроля и оценки результатов обучения**
умения: определять виды угроз безопасности информации и информационных процессов; применять методы защиты информации в компьютерных системах и компьютерных сетях; применять методы криптографической защиты информации; классифицировать компьютерные вирусы и использовать антивирусные программы; проектировать технические средства обеспечения безопасности и применять аппаратно-программные средства защиты информации от НСД; применять правовые нормы защиты информации и информационных процессов. ориентироваться в нестандартных условиях и ситуациях, анализировать возникающие проблемы, разрабатывать и осуществлять план действий.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет
знания: основные угрозы информации в компьютерных системах; специфику возникновения угроз в открытых сетях; основные руководящие документы в области защиты информационных процессов в компьютерных системах; особенности защиты информации на узлах компьютерной сети; основные категории требований к программной и программно-аппаратной реализации средств защиты информации; требования к защите автоматизированных систем от НСД.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет