

Приложение ППСЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2022-2023 уч.г.: Рабочая программа учебной дисциплины ОП 09. Защита информационных процессов в компьютерных системах

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  
2022

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 ОГАОУ «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 ПСССЗ:**

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:**

- 31 основные угрозы информации в компьютерных системах;
- 32 специфику возникновения угроз в открытых сетях;
- 33 основные руководящие документы в области защиты информационных процессов в компьютерных системах;
- 34 особенности защиты информации на узлах компьютерной сети;
- 35 основные категории требований к программной и программно-аппаратной реализации средств защиты информации;
- 36 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 Ворлдскиллс 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 технических 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 лично 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

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



## 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, формирование 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	<b>18/18</b>	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	<b>10/10</b>	
	Основные угрозы информационной безопасности.	2	
Основные принципы формирования режима обеспечения безопасности.	2		
Характеристики изучения протоколов обмена.	2		
Анализ спектра протоколов обмена.	2		
Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и при наличии изолированного компьютера.	2		
Контрольные работы	*		
Тема 2. Методы защиты	Содержание учебного материала	<b>18/18</b>	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 ЛР 10 ЛР 11
	3.	Инженерно-технические методы защиты информационных процессов.	4	
	4.	Программно-аппаратные методы защиты информации.	2	
	5.	Программно-аппаратные методы защиты информационных процессов.	2	
	6.	Защита электронных документов.	6	
	Лабораторные занятия			
	Практические занятия, в том числе в форме практической подготовки		<b>20/20</b>	
		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		<b>12/12</b>	У1-У7 31-36 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		<b>8/8</b>	
	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		<b>12/12</b>	У1-У7 31-36 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	<b>18/18</b>	
		Основные виды работ администрирования серверных систем и приложений.	2	
		Настройка и администрирование сервера.	2	
		Настройка системы безопасности, контроль и отчеты по трафику.	2	
		Настройка системы безопасности, контроль и отчеты по трафику.	2	
		Классическое администрирование.	2	
		Автоматизация управления ПО.	2	
Самостоятельная работа обучающихся		Обеспечение информационной безопасности СУБД.	2	
		Мониторинг сетевых узлов.	2	
		Мониторинг сетевого трафика.	2	
		Изучение материала по литературным источникам: «Предпосылки появления угроз»	<b>10</b>	
		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»			
	Дифференцированный зачет	2\2		
	<b>Всего:</b>	<b>128</b>		

### 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.

##### **Дополнительные источники:**

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

9. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2013.
10. 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.
11. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
12. 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](http://www.fstec.ru)
2. Информационный портал по безопасности [www.SecurityLab.ru](http://www.SecurityLab.ru).
3. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
4. Сайт журнала Информационная безопасность <http://www.itsec.ru> –
5. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)
6. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)
7. (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)

#### **Цифровая образовательная среда СПО PROОбразование:**

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 PROОбразование : [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 с. — ISBN 978-5-4487-0299-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [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
<p><b><u>умения:</u></b>  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.</p> <p><b><u>знания:</u></b>  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.</p>	<p>Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания.  Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет</p> <p>Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания.  Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет</p>