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

Рабочая программа учебной дисциплины

ОП 19. Безопасность информационных систем

для специальности

09.02.07 Информационные системы и программирование

г. Алексеевка
2023

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1547, с учетом профессионального стандарта «Администратор баз данных», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 17 сентября 2014 года № 647н.

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

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность информационных систем

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 09.02.07 Информационные системы и программирование.

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 ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;

У2 анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;

У3 применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.

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

З1объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;

З2понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;

З3базовые составляющие в области развития систем информационной безопасности;

З4классификацию объектов защиты.

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

ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях

ОК 04 Эффективно взаимодействовать и работать в коллективе и команде

ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием

ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания

ПК 7.2. Осуществлять администрирование отдельных компонент серверов

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов 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:

1) 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;

2) 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 - 70 часов, в том числе: аудиторной учебной работы обучающегося - 70 часов, из них в форме практической подготовки – 56 часов; в том числе практических занятий - 50 часов; самостоятельной учебной работы обучающегося - 0 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)	**70**
Аудиторная учебная работа (обязательные учебные занятия) (всего)	**70**
из них в форме практической подготовки	**56**
в том числе:	
лекционные занятия	**20**
лабораторные работы	
практические занятия	**48**
контрольные работы	
Самостоятельная работа обучающегося (всего)	*
Консультации	*
Промежуточная аттестация: *дифференцированный зачет 6 семестр*	**2**

2.2. Тематический план и содержание учебной дисциплины Безопасность информационных систем

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 компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы
1	**2**	**3**	
Тема 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Содержание учебного материала, в том числе в форме практической подготовки	**4/0**	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4 ЛР 4 ЛР 7
	1 Конфигурация сетевой инфраструктуры: настройка хост-машины, сетевого окружения, виртуальных машин, и т.п.	2	
	2 Установка и настройка системы корпоративной защиты от внутренних угроз.	2	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки Установка и настройка агентского мониторинга. Синхронизация с LDAP-сервером, раздел персоны заполнен корректно. Запуск системы корпоративной защиты от внутренних угроз, проверка работоспособности. Имитация процесса утечки конфиденциальной информации в системе.	**8/8** 2 2 2 2	
	Контрольные работы	*	
Тема 2. Исследование (аудит) организации с целью защиты от внутренних угроз	Содержание учебного материала	**4/4**	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4
	1. Угрозы информационной безопасности	2	
	2. Угрозы информационной безопасности	2	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**8/8**	

	Изучение структуры организации на основании полученных материалов («модели организации»), проведение обследования корпоративных информационных систем. Определение объектов защиты, роли пользователей, права доступа. Определение каналов передачи данных и потенциальных утечек. Определение перечня нормативных актов РФ, задействованных в рамках модели угроз информационной безопасности.		ЛР 4 ЛР 7 ЛР 10 ЛР 11
	Контрольные работы	*	
Тема 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	Содержание учебного материала, в том числе в форме практической подготовки	**4/4**	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4 ЛР 4
	1 Политика безопасности	2	
	2 Политики безопасности в системе IWTM	2	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки Разработка и модифицирование политики безопасности, перекрывающие каналы передачи данных и возможные инциденты. Разработка и модификация объектов защиты, категории, технологии защиты в DLP-системе. Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных. Занести политики информационной безопасности в DLPсистему Применение политик для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации.	**10/10**	
Тема 4. Технологии анализа и защиты сетевого трафика	Содержание учебного материала, в том числе в форме практической подготовки	**4/2**	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11
	1 Технологии анализа и защиты сетевого трафика	2	
	2 Межсетевое взаимодействие и туннелированные.	2	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки Развёртывание, настройка и проверка работоспособности VPN-сети на существующей вычислительной инфраструктуре. VPN. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. VPN. Восстановление связи. Обновление ключевой информации. VPN. Централизованные политики безопасности. Защита рабочих мест.	**10/10**	

	IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий		
Тема 5. Технологии агентского мониторинга	Содержание учебного материала, в том числе в форме практической подготовки	**4/0**	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11
	1 Технологии агентского мониторинга	2	
	2	2	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки Разработка и применение политики агентского мониторинга для работы с носителями и устройствами. Разработка и применение политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата	**6/6**	
Тема 6. Анализ выявленных инцидентов	Содержание учебного материала, в том числе в форме практической подготовки	***/***	ОК 01-09 ПК 5.3, 6.4, 7.2, 7.5 У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11
	1 Анализ выявленных инцидентов		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки: Подготовка отчётов о нарушениях. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса. Разработка плана по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.	**6/6**	
	Дифференцированный зачет	**2**	
	Всего:	**70**	

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. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2019-256 с.

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. ГубенковА.А.Информационнаябезопасность 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
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 с. — 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 Профессионалы	**Формы и методы контроля и оценки результатов обучения**
умения: ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности; анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности; применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет
знания: объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности; понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности; базовые составляющие в области развития систем информационной безопасности; классификацию объектов защиты.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет