

МИНИСТЕРСТВО ОБРАЗОВАНИЯ САМАРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

УТВЕРЖДЕНО

Приказ ГБПОУ «ГК г. Сызрани»
от « 31 » марта 2026 г. №78-о

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

основной образовательной программы
по специальности:

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

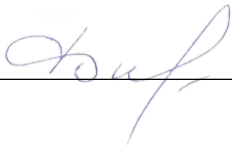
Сызрань, 2026 г.

РАССМОТРЕНА

Предметной (цикловой) комиссией
общепрофессиональных и
профессиональных циклов
председатель М.В. Киреева
от «26 » марта 2026 г. протокол № 7

СОГЛАСОВАНО

ИП Фирсов Е. В.

 Е. В. Фирсов

от «26 » марта 2026 г. протокол № 7

Составитель: М.В. Киреева, преподаватель общепрофессиональных дисциплин строительного
профиля ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная):

И.Н. Ежкова, методист строительного профиля ГБПОУ «ГК г. Сызрани»

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденной приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 (ред. от 03.07.2024 г.).

Рабочая программа разработана с учетом требований профессионального стандарта (далее – ПС) 06.030 «Специалист по защите информации в автоматизированных системах», 5 уровень квалификации, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25.11.2016 N 44449).

Рабочая программа ориентирована на подготовку студентов к выполнению технических требований демонстрационного экзамена по компетенции Корпоративная защита от внутренних угроз информационной безопасности.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	5
3. СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	6
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	9
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	13
6. ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ	14
ПРИЛОЖЕНИЕ	15

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Область применения программы

Рабочая программа производственной практики (далее производственная практика) профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами является частью основной образовательной программы подготовки специалистов среднего звена (далее - ППССЗ) в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем базовой подготовки в части освоения основного вида профессиональной деятельности (далее ВПД) - Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих общих (далее ОК) и профессиональных компетенций (далее ПК).

1.2. Цели и задачи производственной практики

Цель производственной практики – приобретение обучающимися практического опыта, формирование компетенций в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения указанным видом профессиональной деятельности и соответствующими ПК обучающийся в ходе прохождения производственной практики ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами должен:

иметь практический опыт:

- установки, настройки программных средств защиты информации;
- тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;
- учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

1.3. Количество часов на освоение программы производственной практики

Всего – 144 часа (4 недели).

Итоговая аттестация проводится за счет времени, отведенного на производственную практику.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Результатом освоения обучающимися рабочей программы производственной практики является приобретенный практический опыт, сформированные ПК в рамках ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами в соответствии с указанным видом профессиональной деятельности:

Код	Наименование результата освоения практики
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
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.

В процессе освоения ПМ обучающиеся овладевают ОК:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, 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.	Использовать информационные технологии в профессиональной деятельности.

ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

3. СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Задания на практику

Код и наименование ПК	Задания на практику
ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Заполнять ежедневно дневник о ходе прохождения производственной практики; Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Анализ принципов построения систем информационной защиты производственных подразделений.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Заполнять ежедневно дневник о ходе прохождения производственной практики; Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Заполнять ежедневно дневник о ходе прохождения производственной практики; Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	Заполнять ежедневно дневник о ходе прохождения производственной практики; Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Заполнять ежедневно дневник о ходе прохождения производственной практики; Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных	Заполнять ежедневно дневник о ходе прохождения производственной практики;

(информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»): Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.
--	---

3.2 Содержание производственной практики

Наименование разделов, тем	Содержание работ производственной практики	Объем часов
Раздел 1. Организация (предприятие) – база прохождения практики	Инструктаж по технике безопасности и пожарной безопасности. Поиск, анализ, обработка информации, подбор профессиональной документации, выбор информационных технологий и способов решения профессиональных задач	12
Раздел 2. Осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации.	Анализ принципов построения систем информационной защиты производственных подразделений.	12
Раздел 3. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	24
Раздел 4. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	24
Раздел 5.Осуществлять обработку, хранение и	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	24

передачу информации ограниченного доступа		
Раздел 6. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	30
Раздел 7. 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	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	12
	Дифференцированный зачет	6
	Всего	144

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

4.1. Организация практики

Производственная практика проводится в организациях на основе договоров, заключаемых между профессиональными образовательными организациями (далее – ПОО) и организациями.

Сроки проведения практики устанавливаются образовательной организацией в соответствии с основной образовательной программой среднего профессионального образования.

Производственная практика ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами проводится под непосредственным руководством и контролем руководителей производственной практики от организаций и ПОО.

ПОО осуществляет руководство практикой, контролирует реализацию программы практики и условия проведения практики организациями, в том числе требования охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми, формируют группы в случае применения групповых форм проведения практики.

Направление на практику оформляется распорядительным актом директора или иного уполномоченного им лица ПОО с указанием закрепления каждого обучающегося за организацией, а также с указанием вида и сроков прохождения практики.

Продолжительность рабочего дня обучающихся должна соответствовать времени, установленному трудовым законодательством Российской Федерации для соответствующих категорий работников, но не более 36 академических часов в неделю.

На период производственной практики обучающиеся приказом по предприятию/учреждению/организации могут зачисляться на вакантные места, если работа соответствует требованиям программы производственной практики, и включаться в списочный состав предприятия/учреждения/организации, но не учитываться в их среднесписочной численности.

С момента зачисления обучающихся на рабочие места на них распространяются требования стандартов, инструкций, правил и норм охраны труда, правил внутреннего трудового распорядка и других норм и правил, действующих на предприятии, учреждении, организации по соответствующей специальности и уровню квалификации рабочих.

За время производственной практики обучающиеся должны выполнить задания на практику в соответствии с данной рабочей программой.

4.2. Требования к минимальному материально-техническому обеспечению производственной практики

Производственная практика проводится в организациях/предприятиях, оснащенных современным оборудованием, использующих современные информационные технологии, имеющих лицензию.

4.3. Информационное обеспечение обучения

Основные источники

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.
2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
3. 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.
4. 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.
5. 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
6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учеб- ное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
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.

Дополнительные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов.-М.:МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова.– М.: МЦНМО, 2006 г
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. 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».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
11. 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.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

4.4. Кадровое обеспечение образовательного процесса

Учебная практика проводится мастерами производственного обучения и (или) преподавателями дисциплин профессионального цикла.

Требования к квалификации педагогических кадров - в соответствии с требованиями действующего федерального государственного образовательного стандарта.

4.5. Требования к организации аттестации и оценке результатов производственной практики

В период прохождения производственной практики обучающимся ведется дневник практики. По результатам практики обучающимся составляется отчет, который утверждается организацией.

В качестве приложения к дневнику практики обучающийся оформляет *графические материалы* подтверждающие практический опыт, полученный на практике.

По итогам практики руководителями практики от организации и от образовательной организации формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, характеристика организации на обучающегося по освоению общих компетенций в период прохождения практики.

Аттестация производственной практики проводится в форме дифференцированного зачета в последний день производственной практики на базах практической подготовки/в учебно-производственной мастерской.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Результаты обучения (практический опыт в рамках ВПД)	Основные показатели оценки результата	Формы и методы контроля и оценки результатов обучения
Установка, настройка программных средств защиты информации	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	- экспертное наблюдение за выполнением работ на практике (за продуктом деятельности и процессом деятельности); - дифференцированный зачет по практике (защита отчета по практике); - квалификационный экзамен (оценивается в процессе выполнения комплексного практического задания)
Тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	- экспертное наблюдение за выполнением работ на практике (за продуктом деятельности и процессом деятельности); - дифференцированный зачет по практике (защита отчета по практике); - квалификационный экзамен (оценивается в процессе выполнения комплексного практического задания)
Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	- экспертное наблюдение за выполнением работ на практике (за продуктом деятельности и процессом деятельности); - дифференцированный зачет по практике (защита отчета по практике); - квалификационный экзамен (оценивается в процессе выполнения комплексного практического задания)
		Дифференцированный зачет

6. ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

Дата актуализации	Результаты актуализации	Фамилия И.О. и подпись лица, ответственного за актуализацию

ПРИЛОЖЕНИЕ

Ведомость соотнесения¹ требований профессионального стандарта по профессии 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Обобщенная трудовая функция (ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ)	Вид профессиональной деятельности (ФГОС СПО)
Формулировка ОТФ: Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД	Формулировка ВПД: Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Трудовые функции	ПК
Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

Требования ПС	Образовательные результаты ФГОС СПО по ПМ	Содержание
Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. 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	

¹ Ведомость соотнесения включается в данную программу на усмотрение ПОО, т.к. содержится в программе ПМ.

Требования ПС	Образовательные результаты ФГОС СПО по ПМ	Содержание
Трудовые действия	Практический опыт	Виды работ на практике
Текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями	установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и ассиметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе.	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Составление документации по учету, обработке, хранению и передаче конфиденциальной информации Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства