

МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КРАСНОЯРСКИЙ КОЛЛЕДЖ ОТРАСЛЕВЫХ ТЕХНОЛОГИЙ И
ПРЕДПРИНИМАТЕЛЬСТВА»

РАССМОТРЕНО
методической комиссией
протокол № 10 от 18.06.2026

УТВЕРЖДЕНО
Директор КГАПОУ «ККОТиП»
_____/Н. В. Журова/
Приказ № 01-55-1п от 29.06.2026

ПРОГРАММА ПОДГОТОВКИ
СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА

09.02.12 Техническая эксплуатация и сопровождение информационных систем
на базе основного общего образования

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНЫХ РАБОТ

Зам. директора по УР
_____/Беспёрстова И.В. /
Подпись ФИО

Красноярск, 2026

СОДЕРЖАНИЕ

1. Пояснительная записка.....	3
2 Критерии оценки результатов самостоятельной работы	4
3 Перечень самостоятельных работ	5
4 Правила оформления работ	6

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации для организации самостоятельной работы по программе учебной дисциплины **ОП.06 Основы информационной безопасности** предназначены для обучающихся по специальности **09.02.12 «Техническая эксплуатация и сопровождение информационных систем»**.

Изучение программы учебной дисциплины **ОП.06 Основы информационной безопасности**, помимо приобретения теоретических знаний и практических умений в ходе аудиторных занятий, предполагает организацию и проведение самостоятельной работы обучающихся.

Самостоятельная работа обучающихся определяется содержанием программы учебной дисциплины **ОП.06 Основы информационной безопасности**, выполняется обучающимися во время учебных занятий по заданию преподавателя без его непосредственного участия.

Самостоятельная работа направлена на освоение обучающимися следующих результатов обучения согласно ФГОС специальности **09.02.12 «Техническая эксплуатация и сопровождение информационных систем»** и требованиям рабочей программы учебной дисциплины **ОП.06 Основы информационной безопасности**.

умения	Применять основные методы и средства защиты информации. Обеспечивать защиту информации в автоматизированных системах. Соблюдать требования нормативных правовых актов в области информационной безопасности. Использовать антивирусные средства и межсетевое экранирование. Анализировать угрозы информационной безопасности и выбирать способы их нейтрализации.
знания	Сущность и основные понятия информационной безопасности. Классификацию угроз информации и методы их предотвращения. Правовые основы и организационные меры защиты информации. Принципы работы криптографических средств защиты. Основы защиты информации в компьютерных сетях. Нормативно-правовую базу в области защиты персональных данных.

Самостоятельная работа формирует и развивает общие и профессиональные компетенции:

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 правовой и 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 российских духовно-нравственных 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.

Код	Наименование общих компетенций
ПК 1.1	Осуществлять сбор данных для выявления требований к типовой информационной системе в соответствии с техническим заданием

2 КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Критериями оценок результатов самостоятельной работы являются:

- уровень освоения студентом учебного материала;
- умение использовать теоретические знания при выполнении практических, ситуационных задач;
- сформированность общеучебных умений;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- уровень самостоятельности студента при выполнении СР.

В соответствии с программой учебной дисциплины **ОП.06 Основы информационной безопасности** по специальности **09.02.12 «Техническая эксплуатация и сопровождение информационных систем»** на самостоятельную работу обучающихся выделено **2 академических часа**.

Задания из перечня самостоятельных работ обучающиеся выполняют индивидуально при консультационно-координирующей помощи преподавателя.

Основная цель самостоятельной работы обучающихся состоит в овладении фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности.

Задачами организации самостоятельной работы обучающихся являются:

- развитие способности работать самостоятельно, формирование самостоятельности мышления и принятия решений;
- развитие активности и познавательных способностей обучающихся, развитие исследовательских умений;
- стимулирование самообразования и самовоспитания;
- развитие способности планировать и распределять свое время.

3 ПЕРЕЧЕНЬ САМОСТОЯТЕЛЬНЫХ РАБОТ

Раздел, тема	Формы и виды самостоятельной работы	Ход выполнения	Кол-во часов	Сроки выполнения и сдачи работы
Раздел 2. Организационно-технические меры защиты	Подготовка реферата	Выбрать тему проекта. Прочитать дополнительную литературу, раскрывающую выбранную тему. Изучить литературу, раскрывающую выбранную тему. Проработать план реферата по выбранной теме. Составить содержание реферата, раскрывающее тему. Оформить реферат по требованиям оформления текстовых документов. Защитить выполненную работу	1*	апрель
Раздел 3. Безопасность в цифровой среде	Подготовка сообщения	Выбрать тему проекта. Прочитать дополнительную литературу, раскрывающую выбранную тему. Изучить литературу, раскрывающую выбранную тему. Проработать план реферата по выбранной теме. Составить содержание реферата, раскрывающее тему. Оформить реферат по требованиям оформления текстовых документов. Защитить выполненную работу	1*	май
Итого			2	

4 ПРАВИЛА ОФОРМЛЕНИЯ РАБОТ

Требования к оформлению рефератов и сообщений

Оформление реферата (сообщения):

1. Формулирование темы. Тема должна быть не только актуальной по своему значению, но оригинальной, интересной по содержанию.
2. Подбор и изучение основных источников по теме (не менее 8-10 источников для реферата, 2-3 источника для сообщения).
3. Составление библиографии.
4. Обработка и систематизация информации.
5. Разработка плана реферата.
6. Написание реферата.
7. Публичное выступление с результатами исследования.

Содержание реферата (сообщения) должно отражать:

1. Знание современного состояния проблемы;
2. Обоснование выбранной темы;
3. Использование известных результатов и фактов;
4. Полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой;
5. Актуальность поставленной проблемы;
6. Материал, подтверждающий научное, либо практическое значение в настоящее время.

Компоненты содержания:

1. Титульный лист.
2. План-оглавление (в нем последовательно излагаются название пунктов реферата, указываются страницы, с которых начинается каждый пункт).
3. Введение (формулируется суть исследуемой проблемы, обосновывается выбор темы, определяется ее значимость и актуальность выбранной темы, указывается цель и задачи реферата, дается анализ использованной литературы).
4. Основная часть (каждый раздел, доказательно раскрывая отдельную проблему или одну из её сторон, логически является продолжением предыдущего, даются все определения понятий, теоретические рассуждения, исследования автора или его изучение проблемы).
5. Заключение (подводятся итоги или дается обобщенный вывод по теме реферата, предлагаются рекомендации).
6. Список литературы (в соответствии со стандартами).

Требования к оформлению реферата (сообщения):

1. Работа оформляется на белой бумаге (формат А4) на одной стороне листа.
2. На титульном листе указывается Ф.И.О. автора, название образовательного учреждения, тема реферата, Ф.И.О. преподавателя (приложение № 1)
3. Обязательно в реферате должны быть ссылки на используемую литературу.
4. Должна быть соблюдена последовательность написания библиографии.
5. Приложения: чертежи, рисунки, графики оформляются черной пастой. Они не входят в общий объем работы
6. Объем реферата: 10-15 листов машинописного текста (без учета титульного листа, списка ключевых слов, содержания, списка использованных источников и приложений).

Темы для написания реферата(сообщения)

1. Эволюция угроз информационной безопасности в XXI веке.
2. Сравнительный анализ симметричных и асимметричных алгоритмов шифрования.
3. Социальная инженерия как основной вектор современных кибератак.
4. Правовое регулирование защиты персональных данных в РФ.
5. Методы биометрической аутентификации: перспективы и уязвимости.
6. Криптовалюты и безопасность: риски и меры защиты.

7. Анализ современных антивирусных решений (сравнительный обзор).
8. Угрозы информационной безопасности в облачных сервисах.
9. Роль межсетевого экранирования в обеспечении безопасности корпоративных сетей.
10. Организационные меры защиты информации на предприятии.
11. Фишинг и методы противодействия.
12. DDoS-атаки: виды, последствия, защита.
13. Безопасность мобильных устройств и приложений.
14. Информационная безопасность в системах дистанционного банковского обслуживания.
15. Виды вредоносного программного обеспечения и их классификация.
16. Принципы работы VPN-технологий и их роль в защите данных.
17. Криптографическая защита электронной почты.
18. Защита информации от несанкционированного доступа.
19. Инциденты информационной безопасности: классификация и порядок реагирования.
20. Роль резервного копирования в стратегии обеспечения непрерывности бизнеса.
21. Компьютерные преступления и ответственность по законодательству РФ.
22. Авторское право в цифровой среде: защита и нарушение.
23. Этические аспекты сбора и обработки персональных данных.
24. Хакеры и хактивизм: мотивация, методы, последствия.
25. Спам: история, правовое регулирование и методы борьбы.
26. Цифровая гигиена: правила безопасного поведения в Интернете.
27. Проблема кибербуллинга и методы ее профилактики.
28. Интернет-зависимость: признаки, последствия, профилактика.
29. Политика безопасности организации: разработка и внедрение.
30. Роль ФСТЭК и Роскомнадзора в обеспечении информационной безопасности.

Критерии оценивания реферата:

Активность	Своевременность и успешность выполнения реферата (сообщения)	Качество усвоенного материала	Творческая составляющая	Перевод баллов в оценку
Посещение занятий без пропусков – 10 баллов	Своевременно выполнена работа- 10 баллов	Точность выполнения работы – 10 баллов	Защита работы аудиторно – 20 баллов	70 б – оценка «5» 40-60 б – оценка «4» 30 баллов – оценка «3» Менее 20 баллов – оценка «2»
	Досрочно выполненная работа – 20 баллов	Эстетичность выполнения работы – 10 баллов	Защита своей работы персонально – 10 баллов	
	Не своевременно выполнена работа – 0 баллов	Полное содержание выполненной работы – 10 баллов	Оформление своей работы несколькими способами – 20 баллов	

Образец титульного листа реферата

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КРАСНОЯРСКИЙ КОЛЛЕДЖ ОТРАСЛЕВЫХ
ТЕХНОЛОГИЙ И ПРЕДПРИНИМАТЕЛЬСТВА»**

РЕФЕРАТ

«(Наименование темы)»

Преподаватель:

Студент:

Группа:

КРАСНОЯРСК, 20__

Информационные источники

Печатные издания:

1. Баринов А.И., Козырев А.А. Информационная безопасность: учебник для среднего профессионального образования. – М.: Академия, 2024. – 288 с.
2. Романов О.А., Семенов С.В. Основы защиты информации: учебное пособие для СПО. – М.: ИНФРА-М, 2025. – 312 с.
3. Макаров О.Ю. Правовое обеспечение информационной безопасности: учебник. – М.: КноРус, 2024. – 256 с.
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2023. – 592 с.
5. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие. – М.: Форум, 2024. – 432 с.

Электронные издания (электронные ресурсы):

6. Информационная безопасность [Электронный ресурс]. – Режим доступа: <http://www.infosecurity.ru>
7. Портал «Безопасность сети» [Электронный ресурс]. – Режим доступа: <http://www.security.ru>
8. Федеральная служба по техническому и экспортному контролю (ФСТЭК) [Электронный ресурс]. – Режим доступа: <http://www.fstec.ru>
9. Национальный центр информационной безопасности [Электронный ресурс]. – Режим доступа: <http://www.ncib.ru>
10. Российское образование. Федеральный портал [Электронный ресурс]. – Режим доступа: <http://www.edu.ru>
11. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]. – Режим доступа: <http://school-collection.edu.ru>
12. Инфоурок. Ведущий образовательный портал России [Электронный ресурс]. – Режим доступа: <https://infourok.ru>
13. Единое окно доступа к образовательным ресурсам [Электронный ресурс]. – Режим доступа: <http://window.edu.ru>

Дополнительные источники:

14. Богданов Д.В., Чугунов А.В. Информационная безопасность компьютерных систем. – СПб.: Питер, 2023. – 368 с.
15. Галатенко В.А. Основы информационной безопасности. – М.: Интернет-Университет Информационных Технологий, 2022. – 264 с.