

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАБАРДИНО – БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ Х.М.БЕРБЕКОВА»**

Колледж информационных технологий и экономики

УТВЕРЖДАЮ

**Директор колледжа информационных
технологий и экономики**



В.Х. Этueva/

« 02 » июня 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Программа подготовки специалистов среднего звена

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Среднее профессиональное образование

**Квалификация выпускника
Техник по защите информации**

Очная форма обучения

Нальчик, 2023 г.

Рабочая программа учебной дисциплины ОП.01 Основы информационной безопасности разработана на основании Федерального государственного образовательного стандарта среднего профессионального образования специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (базовая подготовка), утвержденного приказом Министерства образования и науки РФ от 09.12.2016 г. №1553., учебного плана по программе подготовки специалистов среднего звена Обеспечение информационной безопасности автоматизированных систем.

Разработчик: Дзамихова Ф.Х., преподаватель

Рабочая программа учебной дисциплины рассмотрена и одобрена на заседании ЦК Компьютерных систем, информационной безопасности и разработки электронных устройств

Протокол № 10 от « 01 » июня 2023 г.

Председатель ЦК



Тлупов З.А.

СОДЕРЖАНИЕ

| | |
|---|-----------|
| 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ | 4 |
| 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ | 5 |
| 3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ | 10 |
| 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ | 12 |

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена: общепрофессиональная дисциплина профессионального цикла

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

В результате освоения дисциплины обучающийся должен
уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

В результате освоения учебной дисциплины обучающийся должен формировать общие и профессиональные компетенции:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

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

1.4. Количество часов на освоение рабочей программы учебной дисциплины:

объем образовательной программы учебной дисциплины – 79 часов, в том числе:

объем работы обучающихся с преподавателем – 63

самостоятельная работа - 4

консультации – 6

промежуточная аттестация – 6

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

| Вид учебной работы | Объем часов |
|---|--------------------|
| Объем образовательной программы учебной дисциплины | 79 |
| в том числе: | |
| теоретическое обучение | 45 |
| практические занятия | 18 |
| Самостоятельная работа | 4 |
| Консультация | 6 |
| Промежуточная аттестация в форме экзамена | 6 |

2.2. Тематический план и содержание учебной дисциплины ОП.01 Основы информационной безопасности

| Наименование разделов и тем | Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся | Объем часов | Уровень освоения |
|---|---|-------------|------------------|
| 1 | 2 | 3 | 4 |
| Раздел 1. Теоретические основы информационной безопасности | | | |
| Тема 1.1. Основные понятия и задачи информационной безопасности | Содержание учебного материала | 8 | |
| | Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Требования к защите информации. Обзор защищаемых объектов и систем. | 2 | 1 |
| | Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности. | 2 | 1 |
| | <i>Практические занятия</i> | | |
| | Международные стандарты информационного обмена. | 4 | 2 |
| | Требования к защите информации | | |
| Тема 1.2. Основы защиты информации | Содержание учебного материала | 12 | |
| | Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. | 8 | 1 |
| | Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. | | |
| | Цели и задачи защиты информации. Основные понятия в области защиты информации. | | |
| | Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности. | | |
| | <i>Практические занятия</i> | | |
| | Определение объектов защиты на типовом объекте информатизации. | 4 | 2 |
| | Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | | |

| | | | |
|--|---|----|---|
| | Самостоятельная работа: Подготовка отчетов по практическим занятиям | 2 | 3 |
| | Рубежный контроль №1. | 1 | |
| Тема 1.3. Угрозы безопасности защищаемой информации. | Содержание учебного материала | 12 | |
| | Понятие угрозы безопасности информации. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Причины нарушения целостности информации. | 8 | 1 |
| | Системная классификация угроз безопасности информации. | | |
| | Каналы и методы несанкционированного доступа к информации | | |
| | Уязвимости. Методы оценки уязвимости информации | | |
| | Практическое занятие | | |
| | Определение угроз объекта информатизации и их классификация | 4 | 2 |
| | Методы несанкционированного доступа к информации | | |
| Раздел 2. Методология защиты информации | | | |
| Тема 2.1. Методологические подходы к защите информации | Содержание учебного материала | 4 | 1 |
| | Анализ существующих методик определения требований к защите информации. | 4 | |
| | Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. | | |
| | Виды мер и основные принципы защиты информации. | | |
| Тема 2.2. Нормативно правовое регулирование защиты информации | Содержание учебного материала | 10 | |
| | Организационная структура системы защиты информации | 8 | 1 |
| | Законодательные акты в области защиты информации. | | |
| | Российские и международные стандарты, определяющие требования к защите информации. | | |
| | Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации | | |
| | Практическое занятие | | |
| | Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности | 2 | 2 |
| Тема 2.3. Защита информации в автоматизированных (информационных) системах | Содержание учебного материала | 15 | 1 |
| | Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. | 11 | |
| | Программные и программно-аппаратные средства защиты информации | | |
| | Инженерная защита и техническая охрана объектов информатизации | | |
| | Организационно-распорядительная защита информации. Работа с кадрами и | | |

| | | | |
|--|--|----|---|
| | внутриобъектовый режим. Принципы построения организационно-распорядительной системы. | | |
| | <i>Практическое занятие</i> | | |
| | Выбор мер защиты информации для автоматизированного рабочего места | 4 | |
| | Программные и программно-аппаратные средства защиты информации | | |
| | <i>Самостоятельная работа:</i> Подготовка отчетов по практическим занятиям | 2 | 3 |
| | Рубежный контроль №2. | 1 | |
| | Консультация | 6 | |
| | Промежуточная аттестация | 6 | |
| | Всего | 79 | |

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

3.2. Информационное обеспечение обучения

3.2.1 Основные печатные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2015.

3.2.2 Дополнительные печатные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2006. - 544 с.: ил. Допущено УМО ИБ.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М.: КНОРУС, 2016.

5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

6. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.

7. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2015.

8. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - М.: Академия. 2012.

9. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

10. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

3.2.3 Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

3.2.4 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Справочно-правовая система «Консультант Плюс» www.consultant.ru
4. Справочно-правовая система «Гарант» » www.garant.ru
5. Федеральный портал «Российское образование» www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
7. Российский биометрический портал www.biometrics.ru
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» [http\\:www.ict.edu.ru](http://www.ict.edu.ru)
9. Сайт Научной электронной библиотеки www.elibrary.ru
10. ЭБС «Лань» <https://e.lanbook.com/>
11. ЭБС «IPRbooks» <http://iprbookshop.ru/>
12. ЭБС «Юрайт» для СПО <https://www.biblio-online.ru/>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, рубежных точек, экзамена.

| Результаты обучения | Формы и методы оценки |
|--|---|
| <p>Знания:</p> <ul style="list-style-type: none">– сущность и понятие информационной безопасности, характеристику ее составляющих;– место информационной безопасности в системе национальной безопасности страны;– виды, источники и носители защищаемой информации;– источники угроз безопасности информации и меры по их предотвращению;– факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;– современные средства и способы обеспечения информационной безопасности;– основные методики анализа угроз и рисков информационной безопасности. | <p>Экспертная оценка знаний студентов во время выполнения:</p> <ul style="list-style-type: none">- практических занятий,- экзаменов,- рубежных точек. |
| <p>Умения:</p> <ul style="list-style-type: none">– классифицировать защищаемую информацию по видам тайны и степеням секретности;– классифицировать основные угрозы безопасности информации. | <p>Экспертная оценка знаний студентов во время выполнения:</p> <ul style="list-style-type: none">- практических занятий,- экзаменов,- рубежных точек. |