МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт–
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.17 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

для студентов колледжа НТИ НИЯУ МИФИ,
обучающихся по программе среднего профессионального образования

специальность 09.02.07
«Информационные системы и программирование»

очная форма обучения
на базе основного общего образования

квалификация
программист

Новоуральск 2023

ОДОБРЕНО:
на заседании
цикловой методической комиссии
информационных технологий
Протокол № 3 от 01.03.2023 г.
Председатель ЦМК ИТ
_____ И.И. Горницкая

Разработана на основе ФГОС СПО (утвержден Приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. № 1547, зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный № 44936), с учетом примерной основной образовательной программы, в соответствии с действующим учебным планом, компетентностной моделью выпускника по специальности 09.02.07 Информационные системы и программирование

Рабочая программа учебной дисциплины ОП.17 «Информационная безопасность» - Новоуральск: Изд-во колледжа НТИ НИЯУ МИФИ, 2023. – 15 с.

АННОТАЦИЯ

Рабочая программа учебной дисциплины ОП.17 «Информационная безопасность» предназначена для реализации программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование СПО в очной форме обучения на базе основного общего образования. Содержит разделы: общая характеристика рабочей программы учебной дисциплины, структура и содержание учебной дисциплины, условия реализации учебной дисциплины, контроль и оценка результатов освоения учебной дисциплины. Определяет объем, содержание, порядок изучения учебной дисциплины, а также способы контроля результатов ее изучения

Разработчик: Горницкая И.И., преподаватель высшей категории, председатель ЦМК информационных технологий
Редактор: Горницкая И.И.

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.17 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» 4

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 5

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 12

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.16 ОХРАНА ТРУДА И ТЕХНИКА БЕЗОПАСНОСТИ В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ» 14

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.17 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1 Место дисциплины в структуре основной профессиональной образовательной программы: Учебная дисциплина «Информационная безопасность» принадлежит к общепрофессиональному циклу.

1.2 Цель и планируемые результаты освоения дисциплины:

Реализация учебной дисциплины предусматривает интенсивную общепрофессиональную подготовку обучающихся с организацией практической подготовки как формы образовательной деятельности при освоении учебной дисциплины в период теоретического обучения, практических занятий, самостоятельной работы.

Код ПК, ОК	Умения	Знания
ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Классифицировать основные угрозы безопасности информации. Регистрировать и анализировать события, выявлять признаки атаки инцидентов информационной безопасности.	Сущность и понятие информационной безопасности, характеристику ее составляющих. Место информационной безопасности в системе национальной безопасности страны. Источники угроз информационной безопасности и меры по их предотвращению. Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи. Современные способы, методы и средства обеспечения ИБ.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**36**
в том числе:	
теоретическое обучение	14
из них практическая подготовка	*4**
практические занятия	20
из них практическая подготовка	*20**
Самостоятельная работа	2
из них практическая подготовка	*2*
Промежуточная аттестация в форме семестрового зачета	**в том числе**

2.2 Тематический план и содержание учебной дисциплины ОП.17 «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Введение	**Содержание учебного материала**	**2**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Специализация учебной дисциплины. Место знаний и умений по учебной дисциплине в структуре ООП СПО по специальности 09.02.07 «Информационные системы и программирование».		
	Формируемые компетенции.		
	Требования к образовательным результатам и результатам обучения студента, содержание и виды учебных занятий и отчетности.		
Раздел 1 Теоретические основы информационной безопасности		**0**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.		

	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.		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**8**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.		
	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.		
	В том числе практических занятий и лабораторных работ Практические занятия: Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		

Тема 1.3. Угрозы безопасности защищаемой информации	**Содержание учебного материала**		ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Понятие угрозы безопасности информации		
	Системная классификация угроз безопасности информации.		
	Уязвимости. Методы оценки уязвимости информации		
	Самостоятельная работа обучающихся Чек-лист: 1 Подготовить устный доклад на тему «Социальная инженерия» 2 В докладе рассмотреть вопросы: -Что такое социальная инженерия? - Значение OSINT (Open Source INTelligence) в социальной инженерии - Цель и задачи социальной инженерии - Методы социальной инженерии - Фишинговые сайты - Почтовые и SMS рассылки, спам - Способы защиты от атак методами социальной инженерии - Как не стать жертвой злоумышленника? 3 К докладу подготовить презентацию - программное обеспечение для разработки презентации по выбору студента	**4**	
	В том числе практических занятий и лабораторных работ Практические занятия: Определение угроз объекта информатизации и их классификация		

Раздел 2 Методология защиты информации		**0**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**	**6**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Анализ существующих методик определения требований к защите информации.		
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.		
	Виды мер и основные принципы защиты информации.		
	В том числе практических занятий и лабораторных работ Практические занятия: Определение угроз объекта информатизации и их классификация		
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	**6**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Организационная структура системы защиты информации		
	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		
	В том числе практических занятий и лабораторных работ Практические занятия: Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		

Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**		ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ОК 09, ПК 4.4, ПК 11.6
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.		
	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		
	Самостоятельная работа обучающихся Чек-лист: 1 Написать эссе на тему «Программно-аппаратные закладки в защищенных информационных системах» - требования к написанию эссе размещены в разделе\Рекомендации и образцы для студентов файл: Рекомендации_по_написанию_Эссе.pdf https://mega.nz/file/KK4EUKIK#R_158jeWid6ZkGgax--3xKb915McdAgWfPNRrcYBXlM 2 На сайте студента по ОП.17 Информационная безопасность создать раздел - Задание к Тема 2.3 «Защита информации в автоматизированных (информационных) системах» 3 Разместить эссе на сайте студента по ОП.17 Информационная безопасность в разделе - Задание к Тема	**6**	

	2.3 «Защита информации в автоматизированных (информационных) системах» 4 Скопировать URL-адрес страницы раздела - Задание к 2.3 «Защита информации в автоматизированных (информационных) системах» сайта по ОП.17 Информационная безопасность 5 Выслать преподавателю URL-адрес сайта для оценивания выполненной работы		
	В том числе практических занятий и лабораторных работ Практические занятия: Выбор мер защиты информации для автоматизированного рабочего места		
Всего:		**36**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория программного обеспечения и сопровождения компьютерных систем, оснащенная необходимым для реализации программы учебной дисциплины оборудованием

– Автоматизированные рабочие места на 12 обучающихся (Intel Core i3, RAM 4 Gb);

– Автоматизированное рабочее место преподавателя (Intel Core i3, RAM 4 Gb);

– Проектор и экран;

– Маркерная доска;

– Программное обеспечение общего и профессионального назначения (Liberica JDK, Python, Apache NetBeans, IntelliJ IDEA, PyCharm, MS VS Code, Atom, 1С:Предприятие (учебная версия), MySQL Workbench, HeidiSQL, DataGrip, SQL Server Management Studio, JDBC Driver for SQL Server, JDBC Driver for PostgreSQL, JDBC Driver for MySQL, MySQL, PostgreSQL, MariaDB, SQLite, OpenServer, XAMPP, Laragon, Mozilla Firefox, Yandex Browser, Atom, Opera, Google Chrome, Blender, SceneBuilder, LibreOffice Draw, MS Office 2016).

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организацией выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Бубнов А. А. Основы информационной безопасности: учебное издание / Бубнов А. А., Пржегорлинский В. Н., Савинкин О. А. - Москва : Академия, 2020. - 256 с.

3.2.2. Основные электронные издания

1 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542339

2 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537691

3 Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510

4 Научно-практический журнал «Безопасность информационных технологий». URL: http://bit.mephi.ru/ (https://bit.spels.ru/index.php/bit)

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.16 ОХРАНА ТРУДА И ТЕХНИКА БЕЗОПАСНОСТИ В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ»

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины: – Сущность и понятие информационной безопасности, характеристику ее составляющих. – Место информационной безопасности в системе национальной безопасности страны. – Источники угроз информационной безопасности и меры по их предотвращению. – Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи. – Современные способы, методы и средства обеспечения ИБ.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят	Формы и методы контроля и оценки – Компьютерное тестирование на знание терминологии по теме; – Тестирование – Контрольная работа – Самостоятельная работа. – Выполнение проекта; – Наблюдение за выполнением практического задания. (деятельностью студента) – Оценка выполнения практического задания(работы) – Подготовка и
Перечень умений, осваиваемых в рамках		

дисциплины: – Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. – Классифицировать основные угрозы безопасности информации. – Регистрировать и анализировать события, выявлять признаки атаки инцидентов информационной безопасности.	существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	выступление с докладом, сообщением, презентацией – Решение ситуационной задачи