

государственное автономное профессиональное образовательное учреждение
Самарской области
«Новокуйбышевский гуманитарно-технологический колледж»



Подписан цифровой
подписью:
Земалиндинова
Венера
Миннихатиповна
Дата: 2025.11.07
16:25:33+04'00'

УТВЕРЖДЕНО
Директор ГАПОУ «НГТК»
В.М. Земалиндинова
Приказ от 03.02.2025 г. № 26-К

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 Основы информационной безопасности

для специальности:

09.02.07 Информационные системы и программирование

профиль подготовки: технический

на базе основного общего образования

РАССМОТРЕНО НА ЗАСЕДАНИИ

Предметно-цикловой комиссии
математики, информационных
технологий и программирования
И.Г. Фролова

ОДОБРЕНО

Заместитель директора
Н.П. Свириденко

Рабочая программа учебной дисциплины ОП.16 Основы информационной безопасности составлена в соответствии с Федеральным государственным образовательным стандартом по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки Российской Федерации № 1547 от 09.12.2016 г., зарегистрированного Министерством юстиции России № 44936 от 26 декабря 2016 г.

Разработчик:

ГАПОУ «НГТК»

(место работы)

преподаватель

(занимаемая должность)

Нагорный А.В.

(инициалы, фамилия)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Основы информационной безопасности» принадлежит к общепрофессиональному циклу.

1.2 Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК	Умения	Знания
ОК 01 - ОК 06 ОК 09 ПК 5.3- ПК 5.7 ПК 9.4 ПК 9.5 ПК 9.8	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации.	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 конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности.

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	80
в т.ч. в форме практической подготовки	48
в том числе:	
теоретическое обучение	32
практические занятия	48
Консультация	2
Экзамен	6

2.2. Содержание учебной дисциплины ОП.16 Основы информационной безопасности

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Код образовательного результата ФГОС СПО
1	2		3	4
Тема 1. Информационная безопасность в системе национальной безопасности РФ	Содержание		8	ОК 01 -ОК 06 ОК 09 ПК 5.3-ПК 5.7 ПК 9.4 ПК 9.5 ПК 9.8
	1	Место информационной безопасности в системе национальной безопасности РФ	6	
	2	Направления государственной политики в области информационной безопасности		
	3	Источники и содержание угроз в информационной сфере		
	Практические занятия		2	
	1	Анализ примеров нарушений информационной безопасности и их последствий		
Тема 2. Законодательная и нормативная база информационной безопасности	Содержание		4	
	1	Законодательство РФ по ИБ, персональные данные, ответственность за нарушения	2	
	Практические занятия		2	
	1	Разбор кейсов нарушения ИБ и юридических последствий		
Тема 3. Криптографические	Содержание		8	
	1	Шифрование: симметричные и асимметричные алгоритмы, хэш-функции	4	

основы защиты информации	2	Электронная подпись, сертификаты, практическое применение	
	Практические занятия		4
	1	Работа с программами шифрования, создание и проверка ЭЦП	
Тема 4. Технические средства и методы защиты	Содержание		6
	1	Антивирусы, фаерволы, IDS/IPS, резервное копирование	2
	Практические занятия		4
	1	Установка и настройка антивируса, фаервола, практика резервного копирования	
Тема 5. Безопасность веб-приложений	Содержание		14
	1	Уязвимости веб-приложений: SQL-инъекции, XSS, CSRF, OWASP Top-10	6
	2	Безопасное программирование и тестирование веб-приложений	
	Практические занятия		8
	1	Поиск и устранение уязвимостей на тестовых стендах, защита форм	
Тема 6. Организационные меры информационной безопасности	Содержание		6
	1	Политики безопасности, управление доступом, обучение пользователей	2
	Практические занятия		4
	1	Разработка политики безопасности организации, создание инструкций	
Тема 7. Практика обеспечения	Содержание		10
	1	Интеграция средств защиты в цикл разработки, DevSecOps	2

информационной безопасности в деятельности веб-разработчика	Практические занятия		8
	1	Настройка защиты на сервере	
	2	Внедрение безопасных практик при разработке	
Тема 8. Резервное копирование и восстановление данных	Содержание		8
	1	Принципы резервного копирования и восстановления, виды резервных копий	2
	Практические занятия		4
	1	Практика резервного копирования веб-проектов, восстановление из копии	
Консультация			4
Экзамен			6
Всего			80

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета и лаборатории.

Оборудование учебного кабинета: стандартное оборудование рабочих мест преподавателя и студента.

Технические средства обучения: персональный компьютер, мультимедиа проектор, экран.

Оборудование лаборатории и рабочих мест лаборатории:

Персональный компьютер и периферийные устройства (принтер, картриджи, сканер, винчестер, CD и DVD-ROM и др.) для проведения практических работ, телекоммуникационные средства.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы 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. Баранова, Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учеб. Пособие. - 3-е изд, перераб. И доп. - Москва : РИОР : ИНФРА-М, 2016 - 322 с. - (Высшее образование).

3.2.2. Дополнительные источники

1. Воронцова, С.В. Обеспечение информационной безопасности в банковской сфере : монография / С.В. Воронцова.- 2-е изд., стер. - Москва : КНОРУС, 2020. - 160 с. - (Legitimitate legen et ordinem).

2. Шаханова, М.В. Современные технологии информационной безопасности : учебнометодический комплекс. - Москва : Проспект, 2020. - 216 с.

3. Ищейнов, В.Я., Мецатунян М.В. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. -Москва : ФОРУМ : ИНФРА- М, 2021. - 208 с. - (Профессиональное образование).

4. Нестеров, С.А. Основы информационной безопасности : Учебное пособие. - 2-е изд., стер. - Санкт-Петербург : Издательство "Лань", 2020. - 324 с. - (Учебник для вузов. Специальная литература).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	Критерии оценки	Методы оценки
Уметь	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при	Проверка конспектов. Проверка выполнения практических задач, тетрадей. Дифференцированный зачет
Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации.		
Знать		
сущность и понятие информационной безопасности, характеристики ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной	видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними дискуссионными навыками и приемами, активно проявляет себя в групповой работе; Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу, излагает его, не	

информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности.	допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении дискуссионных вопросов и задач, владеет необходимыми навыками и приемами их выполнения, способен проявлять себя в групповой работе; Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач, не активен в групповой работе; Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала,	
--	--	--

	допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно, не принимает участие в групповой работе.	
--	---	--