

Приложение
к ОПОП по специальности
10.02.05 Обеспечение
информационной
безопасности
автоматизированных систем

Рабочая программа профессионального модуля

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

**по специальности
среднего профессионального образования
(программа подготовки специалистов среднего звена)**

**10.02.05 Обеспечение информационной безопасности автоматизированных
систем**

Омск, 2025 г.

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Область применения программы

Рабочая программа профессионального модуля «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

Целями освоения профессионального модуля являются:

- освоение студентами основных принципов и методов, применяемых при защите компьютерных систем;
- изучение и практическое освоение технических средств охраны как составной части системы защиты информации;
- обучения основным механизмам защиты современных операционных систем;
- подготовка к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники;
- изучение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачами освоения профессионального модуля являются:

- ознакомить обучающихся с основными проблемами защиты информации в компьютерных системах, а также с основными понятиями, используемыми при защите информации в компьютерных системах;
- обучить обучающихся методам защиты информации в компьютерных системах для построения защищенных информационных технологий;
- знакомить обучающихся с руководящими документами и стандартами в области защиты информации в компьютерных системах;
- дать теоретические основы устройства и функционирования современных операционных систем;
- получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, отработка практических навыков администрирования наиболее распространенных средств защиты, изучение взаимосвязей в работе операционных систем и средств защиты;
- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров.

В результате освоения дисциплины обучающийся должен:

Иметь практический опыт	– 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 асимметричных 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.
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов, и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях от несанкционированного доступа
-------	---

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

.В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
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.
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	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 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	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 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Индекс	Наименование циклов, дисциплин, профессиональных модулей, МДК, практик	Объем образовательной программы (всего)	в т.ч. в форме практической подготовки	Учебная нагрузка обучающегося (час.)						
				самостоятельная работа	во взаимодействии с преподавателем					
					в том числе					промежуточная аттестация
					всего	лекции	практические, лабораторные занятия, семинары	курсовые проекты (работы)	консультации	
ПМ.02	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	586	150	102	244	56	150	24	14	24
МДК.02.01	Программные и программно-аппаратные средства защиты информации	190	68	54	124	26	68	24	6	12
МДК.02.02	Криптографические средства защиты информации	180	82	48	120	30	82	0	8	12
УП.02	Учебная практика	72								
ПП.02	Производственная практика	144								

3.2. Тематический план и содержание профессионального модуля (ПМ)

3.2.1 Тематический план и содержание МДК.02.01 Программные и программно-аппаратные средства защиты информации

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	190
аудиторная учебная нагрузка (всего):	
лекций	26
практических занятий,	68
включая курсовую работу	24
консультации	6
Промежуточная аттестация	12
Самостоятельная работа обучающегося	54
Промежуточная аттестация в форме экзамена	

№ п/п	Тема	Количество часов						
		Всего	Лекции	Практические занятия	Курсовая работа	Консультации	СРС	Промежуточная аттестация
1.	Тема 1.1. Предмет и задачи программно- аппаратной защиты информации	2	2					
2.	Тема 1.2. Стандарты безопасности	6	2	2			2	
3.	Тема 1.3. Защищенная автоматизированная система	6	2	2			2	
4.	Тема 1.4. Дестабилизирующее воздействие на объекты защиты	6	2	2			2	
5.	Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	6	2	2			2	
6.	Тема 2.1. Основы защиты автономных автоматизированных систем	6	2	2			2	
7.	Тема 2.2. Защита программ от изучения	6		2			4	
8.	Тема 2.3. Вредоносное программное обеспечение	6		4			2	
9.	Тема 2.4. Защита программ и данных от несанкционированного копирования	6		4			2	
10.	Тема 2.5. Защита информации на машинных носителях	6		4			2	
11.	Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	6		4			2	
12.	Тема 2.7. Системы обнаружения атак и вторжений	6		4			2	
13.	Консультация	2				2		
	За семестр	70	12	32		2	24	

14.	Тема 3.1. Основы построения защищенных сетей	10	2	4			4	
15.	Курсовая работа	6			6			
16.	Тема 3.2. Средства организации VPN	10	2	4			4	
17.	Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	10	2	4			4	
18.	Курсовая работа	6			6			
19.	Тема 5.1. Защита информации в базах данных	10	2	4			4	
20.	Консультация	2				2		
21.	Тема 6.1. Мониторинг систем защиты	12	2	4			6	
22.	Курсовая работа	6			6			
23.	Тема 6.2. Изучение мер защиты информации в информационных системах	12	2	6			4	
24.	Тема 6.3. Изучение современных программно-аппаратных комплексов.	16	2	10			4	
25.	Курсовая работа	6			6			
26.	Консультация	2				2		
27.	Промежуточная аттестация	12						12
	За семестр	120	14	36	24	4	30	12
	ВСЕГО	190	26	68	24	6	54	12

Раздел 1. Основные принципы программной и программно-аппаратной защиты информации

Тема 1.1. Предмет и задачи программно- аппаратной защиты информации

Предмет и задачи программно-аппаратной защиты информации

Основные понятия программно-аппаратной защиты информации

Классификация методов и средств программно-аппаратной защиты информации

Тема 1.2. Стандарты безопасности

Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)

Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.

Обзор стандартов. Работа с содержанием стандартов

Тема 1.3. Защищенная автоматизированная система

Автоматизация процесса обработки информации

Понятие автоматизированной системы.

Особенности автоматизированных систем в защищенном исполнении.

Основные виды АС в защищенном исполнении.

Методы создания безопасных систем

Методология проектирования гарантированно защищенных КС

Дискреционные модели

Мандатные модели

Учет, обработка, хранение и передача информации в АИС

Ограничение доступа на вход в систему.

Идентификация и аутентификация пользователей
Разграничение доступа.
Регистрация событий (аудит).
Контроль целостности данных
Уничтожение остаточной информации.
Управление политикой безопасности. Шаблоны безопасности
Криптографическая защита. Обзор программ шифрования данных
Управление политикой безопасности. Шаблоны безопасности

Тема 1.4. Дестабилизирующее воздействие на объекты защиты
Источники дестабилизирующего воздействия на объекты защиты
Способы воздействия на информацию
Причины и условия дестабилизирующего воздействия на информацию
Распределение каналов в соответствии с источниками воздействия на информацию

Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа
Понятие несанкционированного доступа к информации
Основные подходы к защите информации от НСД
Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам
Доступ к данным со стороны процесса
Особенности защиты данных от изменения. Шифрование.
Организация доступа к файлам
Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД

Раздел 2. Защита автономных автоматизированных систем

Тема 2.1. Основы защиты автономных автоматизированных систем

Работа автономной АС в защищенном режиме
Алгоритм загрузки ОС. Штатные средства замыкания среды
Расширение BIOS как средство замыкания программной среды
Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды.
Понятие АМДЗ (доверенная загрузка)
Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

Тема 2.2. Защита программ от изучения

Изучение и обратное проектирование ПО
Способы изучения ПО: статическое и динамическое изучение
Задачи защиты от изучения и способы их решения
Защита от отладки.
Защита от дизассемблирования
Защита от трассировки по прерываниям.

Тема 2.3. Вредоносное программное обеспечение

Вредоносное программное обеспечение как особый вид разрушающих воздействий
Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения
Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.
Бот-нет. Принцип функционирования. Методы обнаружения

Классификация антивирусных средств. Сигнатурный и эвристический анализ
Защита от вирусов в "ручном режиме"
Основные концепции построения систем антивирусной защиты на предприятии
Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО

Тема 2.4. Защита программ и данных от несанкционированного копирования
Несанкционированное копирование программ как тип НСД
Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.
Привязка ПО к аппаратному окружению и носителям.
Защитные механизмы в современном программном обеспечении на примере MS Office
Защита информации от несанкционированного копирования с использованием специализированных программных средств
Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)

Тема 2.5. Защита информации на машинных носителях
Проблема защиты отчуждаемых компонентов ПЭВМ.
Методы защиты информации на отчуждаемых носителях. Шифрование.
Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов
Безвозвратное удаление данных. Принципы и алгоритмы.
Применение средства восстановления остаточной информации на примере Foremost или аналога
Применение специализированного программного средства для восстановления удаленных файлов
Применение программ для безвозвратного удаления данных
Применение программ для шифрования данных на съемных носителях

Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей
Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
Устройства Touch Memory

Тема 2.7. Системы обнаружения атак и вторжений
СОВ и СОА, отличия в функциях. Основные архитектуры СОВ
Использование сетевых sniffеров в качестве СОВ
Аппаратный компонент СОВ
Программный компонент СОВ
Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений.
Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.
Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений

Раздел 3. Защита информации в локальных сетях
Тема 3.1. Основы построения защищенных сетей
Сети, работающие по технологии коммутации пакетов
Стек протоколов TCP/IP. Особенности маршрутизации.
Штатные средства защиты информации стека протоколов TCP/IP.
Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

Тема 3.2. Средства организации VPN

Виртуальная частная сеть. Функции, назначение, принцип построения

Криптографические и некриптографические средства организации VPN

Устройства, образующие VPN. Криptomаршрутизатор и криптофильтр.

Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки

Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки

Развертывание VPN

Раздел 4. Защита информации в сетях общего доступа

Тема 4.1. Обеспечение безопасности межсетевого взаимодействия

Методы защиты информации при работе в сетях общего доступа.

Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности

Основные типы firewall. Симметричные и несимметричные firewall.

Уровень 1. Пакетные фильтры

Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.

Уровень 3. Проxy-сервера прикладного уровня

Однохостовые и мультихостовые firewall.

Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций

Требования по сертификации межсетевых экранов

Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.

Изучение различных способов закрытия "опасных" портов

Раздел 5. Защита информации в базах данных

Тема 5.1. Защита информации в базах данных

Основные типы угроз. Модель нарушителя

Средства идентификации и аутентификации. Управление доступом

Средства контроля целостности информации в базах данных

Средства аудита и контроля безопасности. Критерии защищенности баз данных

Применение криптографических средств защиты информации в базах данных

Изучение механизмов защиты СУБД MS Access

Изучение штатных средств защиты СУБД MSSQL Server

Раздел 6. Мониторинг систем защиты

Тема 6.1. Мониторинг систем защиты

Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации

Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25

Классификация отслеживаемых событий. Особенности построения систем мониторинга

Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.

Классификация сетевых мониторов

Системы управления событиями информационной безопасности (SIEM).

Обзор SIEM-систем на мировом и российском рынке.

Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов

Проведение аудита ЛВС сетевым сканером

Тема 6.2. Изучение мер защиты информации в информационных системах

Изучение требований о защите информации, не составляющей государственную тайну.

Изучение методических документов ФСТЭК по применению мер защиты.

Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств, и рекомендаций по их настройке.

Тема 6.3. Изучение современных программно-аппаратных комплексов.

Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов

Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов

Изучение типовых решений для построения VPN на примере VipNet или других аналогов

Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов

Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов

Примерная тематика курсовых работ

1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
5. Проблема защиты информации в облачных хранилищах данных и ЦОДах
6. Защита сред виртуализации.
7. Защита АС по классу [1В/1Б] с использованием [СЗИ от НСД по своему выбору, кроме рассмотренных на парах]
8. Защита АС по классу [1В/1Б] в ОС Linux с использованием [СЗИ от НСД по своему выбору]
9. Защита ИСПДн по уровню защищенности [...] с использованием [СЗИ от НСД по своему выбору]
10. Организация защиты корпоративных мобильных устройств с использованием [Endpoint, MDM решение по своему выбору]
11. Разработка методики обнаружения вредоносной активности в «интернете вещей» (IoT)
13. Реализация аутентификации на основе атрибутов с использованием [программный продукт по своему выбору]
14. Реализация аутентификации с использованием облачных решений [IDaaS по своему выбору]
15. Разработка средства автоматизации управления доступом к информационным ресурсам (система заявок + предоставление по ним доступа в домене)
16. Разработка средства инвентаризации информационных ресурсов и предоставленных прав доступа к ним
17. Сравнительное тестирование программных решений для инвентаризации информационных ресурсов в организации
18. Организация защиты от утечки информации в корпоративной сети с использованием [DLP решение по своему выбору]
19. Организация антивирусной защиты виртуальной инфраструктуры с использованием [корпоративное антивирусное решение по своему выбору]
20. Организация межсетевого экранирования и обнаружения вторжений в виртуальной

инфраструктуре

21. Разработка подходов по организации журналирования и анализа событий аудита в корпоративной инфраструктуре без использования специализированных систем
22. Организация централизованного журналирования и анализа событий аудита с использованием [SIEM решение по своему выбору]
23. Защита программного обеспечения от несанкционированного копирования с использованием решений на базе HASP SRM
24. Защита программного обеспечения от несанкционированного копирования с использованием решений на базе Guardant
25. Разработка методики и программы инструктажа работника по использованию средств и механизмов защиты информации
26. Разработка системы машинного обучения для автоматизированного построения правил WAF/IPS/FW
27. Разработка системы автоматизации OSINT (разведки на основе открытых источников)
28. Шифрование дисков и разделов в Windows
29. Linux-дистрибутивы для форензики

3.2.2 Тематический план и содержание МДК.02.02 Криптографические средства защиты информации

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	180
аудиторная учебная нагрузка (всего):	
лекций	30
практических занятий,	82
включая курсовую работу	-
консультации	8
Промежуточная аттестация	12
Самостоятельная работа обучающегося	48
Промежуточная аттестация в форме экзамена	

№ п/п	Тема	Количество часов						
		Всего	Лекции	Практические занятия	Курсовая работа	Консультации	СРС	Промежуточная аттестация
1.	Тема 1.1. Математические основы криптографии	16	4	8			4	
2.	Тема 2.1. Методы криптографического защиты информации	8	2	4			2	
3.	Тема 2.2. Криптоанализ	8	2	4			2	
4.	Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	8	2	4			2	
5.	Консультация	2				2		
	За семестр	42	10	20		2	10	
6.	Тема 3.1. Кодирование информации. Компьютеризация шифрования.	12	2	6			4	
7.	Тема 3.2. Симметричные системы шифрования	14	2	8			4	
8.	Тема 3.3. Асимметричные системы шифрования	14	2	8			4	
9.	Консультация	2				2		
10.	Тема 3.4. Аутентификация данных. Электронная подпись	18	4	8			6	
11.	Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	16	2	8			6	
12.	Тема 3.6. Криптозащита информации в сетях передачи данных	18	4	8			6	
13.	Консультация	2				2		
14.	Тема 3.7. Защита информации в электронных платежных системах	14	2	8			4	
15.	Тема 3.8. Компьютерная стеганография	14	2	8			4	
16.	Консультация	2				2		
17.	Промежуточная аттестация	12						12
	За семестр	138	20	62		6	38	12
	ВСЕГО	180	30	82		8	48	12

Раздел 1. Математические основы защиты информации

Тема 1.1. Математические основы криптографии

Элементы теории множеств. Группы, кольца, поля.

Делимость чисел. Признаки делимости. Простые и составные числа.

Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа.

Алгоритм Евклида для нахождения НОД.

Отношения сравнимости. Свойства сравнений. Модулярная арифметика.

Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера.

Алгоритм быстрого возведения в степень по модулю.

Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.

Китайская теорема об остатках.

Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений.

Решето Эратосфена.

Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.

Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.

Арифметические операции над большими числами.

Эллиптические кривые и их приложения в криптографии.

Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений

Проверка чисел на простоту

Решение задач с элементами теории чисел.

Раздел 2. Классическая криптография

Тема 2.1. Методы криптографической защиты информации

Классификация основных методов криптографической защиты. Методы симметричного шифрования

Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр

Методы перестановки. Табличная перестановка, маршрутная перестановка

Гаммирование. Гаммирование с конечной и бесконечной гаммами

Применение классических шифров замены

Применение классических шифров перестановки

Применение метода гаммирования

Тема 2.2. Криптоанализ

Основные методы криптоанализа. Криптографические атаки.

Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхoffsа

Перспективные направления криптоанализа, квантовый криптоанализ.

Криптоанализ шифра простой замены методом анализа частотности символов

Криптоанализ классических шифров методом полного перебора ключей

Криптоанализ шифра Вижинера

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии

Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод VBS.

Применение методов генерации ПСЧ

Раздел 3. Современная криптография

Тема 3.1. Кодирование информации. Компьютеризация шифрования.

Кодирование информации. Символьное кодирование. Смысловое кодирование.

Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII
Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация
программно-аппаратных криптографических систем и средств. Изучение современных
программных и аппаратных криптографических средств
Кодирование информации
Программная реализация классических шифров
Изучение реализации классических шифров замены и перестановки в программе CrypTool
или аналоге.

Тема 3.2. Симметричные системы шифрования

Общие сведения. Структурная схема симметричных криптографических систем
Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р
34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4
Изучение программной реализации современных симметричных шифров

Тема 3.3. Асимметричные системы шифрования

Криптосистемы с открытым ключом. Необратимость систем. Структурная схема
шифрования с открытым ключом.
Элементы теории чисел в криптографии с открытым ключом.
Применение различных асимметричных алгоритмов.
Изучение программной реализации асимметричного алгоритма RSA

Тема 3.4. Аутентификация данных. Электронная подпись

Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции.
Алгоритмы цифровой подписи
Применение различных функций хеширования, анализ особенностей хешей
Применение криптографических атак на хеш-функции.
Изучение программно-аппаратных средств, реализующих основные функции ЭП

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

Алгоритмы распределения ключей с применением симметричных и асимметричных схем
Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация
Применение протокола Диффи-Хеллмана для обмена ключами шифрования.
Изучение принципов работы протоколов аутентификации с использованием доверенной
стороны на примере протокола Kerberos.

Тема 3.6. Криптозащита информации в сетях передачи данных

Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.
Криптомаршрутизатор. Пакетный фильтр
Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с
использованием протоколов WPA, WEP.

Тема 3.7. Защита информации в электронных платежных системах

Принципы функционирования электронных платежных систем. Электронные пластиковые
карты. Персональный идентификационный номер
Применение криптографических протоколов для обеспечения безопасности электронной
коммерции.
Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания
одноразовых паролей

Тема 3.8. Компьютерная стеганография

Скрытая передача информации в компьютерных системах. Проблема аутентификации

мультимедийной информации. Защита авторских прав.

Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ

Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

Реализация простейших стеганографических алгоритмов

3.2.3. Учебная практика

Виды работ:

- 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
- Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи

3.2.4. Производственная практика

Виды работ

- Анализ принципов построения систем информационной защиты производственных подразделений.
- Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
- Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
- Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
- Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие кабинета информационной безопасности, лаборатории программных и программно-аппаратных средств защиты информации, лаборатории информационных технологий, сетей и систем передачи информации, программирования и баз данных; компьютерного класса.

Оснащение кабинета информационной безопасности: посадочные места для обучающихся

Рабочее место преподавателя
Мультимедийный проектор,
экран

Оснащение лаборатории программных и программно-аппаратных средств защиты информации: Средство защиты информации от НСД Secret Net верс. 5.0

Комплекс аппаратный СЗИ НСД Аккорд

Система обнаружения вторжений (IDS) Рабочая станция (Celeron) 11 шт
Коммутатор Cisco Catalyst 2960

Проектор, экран

Антивирусный программный комплекс – Kaspersky Endpoint Security 10

ПА СЗИ от НСД, блокировки доступа и нарушения целостности – Комплекс СЗИ НСД

«Аккорд – АМДЗ»

Программные и программно-аппаратные средства обнаружения вторжений –
ПАК

«ViPNet IDS NS1000 и ПО «Snort»

Средства уничтожения остаточной информации в запоминающих устройствах
– ПО

«СГУ-2» ПО «Secret Net 8.0»

Программные средства выявления уязвимостей в автоматизированных системах и средства выч. техники – ПО «XSpider»

Программные средства криптографической защиты информации – «Средство криптографической защиты информации «КриптоПро CSP »

Программные средства защиты среды виртуализации – ПО «СЗИ vGate R2»

Deductor Academic 5.3

Dev-C++

IIS 10.0 Express Nmap

Notepad++ Npcap

Office 2010 Professional Plus Oracle VM VirtualBox 5.1 Project 2010 Professional
PyCharm Community

RAD Studio 2007 Professional.

Проектор, экран

Оснащение лаборатории информационных технологий, сетей и систем передачи информации, программирования и баз данных:

Посадочные места для обучающихся Рабочее место преподавателя

Рабочие места с персональными компьютерами.

Установленное программное обеспечение:

1С: Предприятие 8.3 (учебная версия) Office 2019 Professional Plus
Windows 10 Professional. Маркерная доска

Сервер виртуализации

Сервер с вычислительными модулями Маршрутизатор Cisco ISR 4321

Коммутатор Cisco Catalyst 2960R+24TC-L

Межсетевой экран Cisco ASA 5506

Сварочные аппараты для оптоволокна

Оснащение компьютерного класса:

Рабочие место с персональными компьютерами.

Установленное программное обеспечение:

1С: Предприятие 8.3 (учебная версия), Atom, Code::Blocks, Creative Cloud for
Teams 2019, Free Pascal 3.0,

IntelliJ IDEA Community, Java SE Dev Kit 8, Notepad++, Office 2019 Professional
Plus, PhpStorm 2019,

PyCharm Community, Python 3.7/3.8, Windows 10 Professional

Рабочие места с ноутбуками.

4.2. Информационное обеспечение обучения

Основная литература:

Белов, Е. Б. Организационно-правовое обеспечение информационной
безопасности : учебник. Рек. ФУМО СПО ИБ / Е. Б. Белов, В. Н. Пржегорлинский
.— М. : Издат. центр "Академия", 2020 .— 336 с.

Дополнительная литература:

Ильин, М.Е. Криптографическая защита информации в объектах
информационной инфраструктуры : учебник. Рек. ФУМО / М. Е. Ильин, Т. И.
Калинкина, В. Н. Пржегорлинский

.— М. : Издат. Центр «Академия», 2020 .— 288 с.

Казарин, О. В. Программно-аппаратные средства защиты информации.
Защита программного обеспечения : учебник и практикум для среднего
профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва :
Издательство Юрайт, 2020. — 312 с.

— (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст :
электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449548>

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, 2019. — 342 с. — (Профессиональное образование). — ISBN
978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:
<https://urait.ru/bcode/431080>

Нестеров, С. А. Информационная безопасность : учебник и практикум для
среднего профессионального образования / С. А. Нестеров. — Москва :
Издательство Юрайт, 2019. — 321 с. — (Профессиональное образование). — ISBN
978-5-534-07979-1. — Текст : электронный

// ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/442312>

Программно-аппаратные средства защиты информационных систем : учебное
пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков ;
Министерство образования и науки Российской Федерации, Федеральное

государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=499013>

Ищукова, Е.А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог : Издательство Южного федерального университета, 2016. – 80 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=493059>

Лапони́на, О.Р. Криптографические основы безопасности / О.Р. Лапони́на. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. : ил. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=429092>

Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. – Москва : Издательский дом Высшей школы экономики, 2015. – 574 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=440285>

Периодические издания:

Вестник	информационной	безопасности
https://dlib.eastview.com/browse/publication/84979	Вопросы защиты информации	
https://dlib.eastview.com/browse/publication/93931	Информационная безопасность	
https://dlib.eastview.com/browse/publication/90269	Безопасность информационных технологий	
https://bit.mephi.ru/index.php/bit		

Вопросы кибербезопасности <https://cyberrus.com/>

Журнал о компьютерной технике Chip/ЧИП <https://ichip.ru/>

Электронные источники:

Федеральная служба по техническому и экспортному контролю <https://fstec.ru/>
Информационный портал по безопасности <https://www.securitylab.ru/> Федеральный портал «Российское образование» <https://edu.ru/>

Справочно-правовая система «КонсультантПлюс»

4.3. Общие требования к организации образовательного процесса

В преподавании дисциплины используются следующие образовательные технологии: лекции; лабораторный практикум. В активной и интерактивной форме проводятся следующие занятия:

Интерактивные лекции-консультации Интерактивные проблемные лекции

Интерактивные практические занятия-семинары в форме деловой игры
Компьютерные симуляции

Разбор конкретных практических ситуаций Психологические и иные тренинги

Лабораторный практикум так же является интерактивной формой проведения занятий, поскольку во время таких занятий происходит постоянное взаимодействие по каналам педагогических коммуникаций преподаватель <=> студент и студент <=> студент. При организации образовательного процесса, в условиях реализации компетентностного подхода предусматривается использование активных форм проведения занятий, в том числе может быть реализовано с применением

электронного обучения и дистанционных образовательных технологий. Кроме того, в процессе преподавания дисциплины используются следующие образовательные технологии:

- выполнение заданий под руководством преподавателя в компьютерном классе (форма занятия – лабораторные занятия);
- мозговой штурм (интерактивная методика) (форма занятия – лекция);
- обмен опытом (форма занятия – лекция);
- наглядная демонстрация (форма занятия – лабораторные занятия);
- обсуждение конкретных ситуаций (интерактивная методика) (форма занятия – лабораторные занятия);
- работа в группах (workshops) (интерактивная методика) (форма занятия – лабораторные занятия);
- обсуждение критического явления (интерактивная методика) (форма занятия – лекция).

Внеаудиторная работа обучающихся предполагает вопросы, тематические эссе, аналитическую обработку отчетов, составление расчетно-аналитических таблиц, подготовку сообщений к выступлению на семинаре, подготовку докладов.

Кроме того, что обучающиеся в рамках самостоятельной внеаудиторной работы для овладения знаниями должны осуществлять чтение текстов (учебника и дополнительной литературы), составление плана текста, конспектирование текстов, делать необходимые выписки, работать со словарями и справочниками, знакомится и изучать нормативные документы; для закрепления и систематизации знаний должны работать с конспектами лекций, отвечать на контрольные вопросы, осуществлять аналитическую обработку текстов (аннотирование, рецензирование, реферирование, контент-анализ); для формирования умений студенты должны решать задачи. Задания для внеаудиторной работы обучающихся включают также составление таблиц, обеспечивающих ознакомление обучающихся с нормативными документами и требующих от студентов их изучения, а также осуществить их аналитическую обработку.

Практическая подготовка организуется в учебных и структурных подразделениях колледжа, а также в специально оборудованных помещениях (рабочих местах) профильной организации на основании договора о практической подготовке обучающихся № 5 от 22 сентября 2020 г. с федеральным государственным образовательным учреждением высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)».

4.4. Кадровое обеспечение образовательного процесса

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности,

указанной в пункте 1.5 настоящего ФГОС СПО, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации	Проявлять знания, навыки и умения в обработке, хранении и передаче	тестирование, экзамен квалификационный, экспертное наблюдение

ограниченного доступа.	информации ограниченного доступа	выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Код и наименование общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов, и способов решения профессиональных задач; адекватная оценка и самооценка эффективности выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 02. Использовать современные	использование различных	программы

средства поиска, анализа и источников, включая интерпретации информации, и электронные ресурсы, медиа информационные технологии для ресурсов, Интернет- ресурсы, выполнения задач периодические издания по профессиональной деятельности специальности для решения профессиональных задач	Экспертное наблюдение и оценка
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	демонстрация на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	ответственности за принятые решения обоснованность самоанализа коррекция результатов собственной работы; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	взаимодействие с обучающимися, преподавателями в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)
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	грамотность устной и письменной речи, ясность формулирования и изложения мыслей
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных	соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих

ситуациях	технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования профессиональной деятельности необходимой технической документации, в том числе на иностранном языке.	