



Автономная некоммерческая организация высшего образования
«Университет ИТ ХАБ» (АНО ВО «Университет ИТ ХАБ»)
115093, Москва, вн. тер. г. Муниципальный округ Даниловский, ул.
Дубининская, д. 96, ОГРН 1257700014362, ИНН 9725176632, КПП
772501001
+7 (499) 350-66-04, +7 (926) 729-08-05; university@ithub.ru, univerithub.ru

«УТВЕРЖДЕНО»

Ректор

АНО ВО «Университет ИТ ХАБ»

Емельянов А.С.

15.06.2026



ДОПОЛНИТЕЛЬНАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности: Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности

Трудоемкость: 1286 часов

Срок обучения: 80 недель

Форма обучения: Очно-заочная с применением ДОТ

Режим занятий: 17 часов в неделю

Москва, 2026

Программа разработана в соответствии с требованиями:

- приказом Министерства науки и высшего образования Российской Федерации от 24 марта 2025 г. № 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам",
- Методических рекомендаций по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов, утвержденными Министерством образования и науки РФ 22.01.2015 № ДЛ-1/05вн.

Содержание программы учитывает требования профессионального стандарта 06.032 Специалист по безопасности компьютерных систем и сетей, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н и федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427

Разработчики:

Руководитель образовательной программы Информационная безопасность

СОДЕРЖАНИЕ

	Общая характеристика программы	4
1	Цель программы	5
2	Планируемые результаты обучения	6
3	Учебный план	10
4	Формы аттестации, оценочные материалы и критерии оценивания результатов обучения	11
5	Организационно-педагогические условия реализации программы	14
Приложение 1. Рабочие программы учебных дисциплин, практики		
Приложение 2. Программа итоговой аттестации		

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Программа профессиональной переподготовки «Сетевые системы и защита данных», является дополнительной профессиональной программой и представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестаций, разработанный и утвержденный АНО ВО «Университет ИТ ХАБ» с учетом потребностей общероссийского и регионального рынка труда.

Программа разработана на основе следующих нормативных документов:

- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. №197-ФЗ (в редакции от 14.07.2022 №283-ФЗ);
- Федеральный закон от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации» (в редакции от 23.07.2025 N 253-ФЗ);
- Приказ Министерства труда и социальной защиты Российской Федерации от 12 апреля 2013 г. №148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;
- Приказ Министерства науки и высшего образования Российской Федерации от 24 марта 2025 г. № 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам";
- Квалификационный справочник должностей руководителей, специалистов и других служащих 4-е издание, дополненное, утвержденного постановлением Минтруда РФ от 21 августа 1998 г. N 37;
- Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «06.032 Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н
- Статья 76. Дополнительное профессиональное образование Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ (в редакции от 14.07.2022 N 301-ФЗ);
- Устав АНО ВО «Университет ИТ ХАБ»;
- Положение О разработке и реализации дополнительных профессиональных программ в АНО ВО «Университет ИТ ХАБ»;
- Порядок проведения Итоговой аттестации по дополнительным профессиональным программам.

Срок обучения составляет 2 года (80 недель). Программа профессиональной переподготовки «Сетевые системы и защита данных» содержит рабочие программы учебных дисциплин: 17 обязательных дисциплин (приложение 1) и итоговой аттестации (приложение 2).

ПЕРЕЧЕНЬ ОПРЕДЕЛЕНИЙ И СОКРАЩЕНИЙ

СПО – среднее профессиональное образование

ВО – высшее образование

ДПП – дополнительная профессиональная программа

ОК – общие (общекультурные) компетенции

ОПК – общепрофессиональные компетенции

ОТФ – обобщенная трудовая функция

ПК – профессиональные компетенции

ПС – профессиональный стандарт

ПСК – профессионально-специализированные компетенции

ТФ – трудовая функция

УК – универсальные компетенции

ФГОС – федеральный государственный образовательный стандарт

1.1. Цель программы

Целью настоящей программы является подготовка квалифицированных специалистов, обладающих глубокими знаниями и навыками в области обеспечения безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности.

1.2. Требования к слушателям

К освоению программы профессиональной переподготовки допускаются:

- лица, имеющие высшее образование в области информационных технологий.
- лица, имеющие непрофильное высшее образование или получающие высшее образование.
- лица, имеющие или получающие среднее профессиональное образование в области Информационных технологий.

1.3. Связь дополнительной профессиональной программы с профессиональными стандартами

Наименование программы	Наименование выбранного профессионального стандарта (одного или нескольких), ОТФ и (или) ТФ	Уровень квалификации ОТФ и (или) ТФ
«Сетевые системы и защита данных»	ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ 06.032 Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н	ОТФ А5. Техническое обслуживание средств защиты информации в компьютерных системах и сетях А/01.5 — техническое обслуживание программно-аппаратных средств защиты информации в операционных системах А/02.5 — техническое

		обслуживание программно-аппаратных средств защиты информации в компьютерных сетях А/03.5 — техническое обслуживание средств защиты информации прикладного и системного ПО
--	--	--

Сопоставление описания квалификации в профессиональном стандарте с требованиями к результатам подготовки по ФГОС ВО

Профессиональный стандарт	УРОВЕНЬ ВО НАПРАВЛЕНИЕ ПОДГОТОВКИ
Трудовые функции: А/01.5 А/02.5 А/03.5	10.03.01 Информационная безопасность

1.4. Планируемые результаты обучения

Выпускник, освоивший профессиональную программу дополнительного образования (профессиональной переподготовки), должен обладать компетенциями, позволяющим выполнять трудовые функции Специалиста по информационным системам.

Перечень компетенций, формируемых в процессе освоения программы соотнесенных с ФГОС ВО представлен в таблице.

Перечень компетенций, формируемых в процессе освоения программы соотнесенных с ФГОС ВО

Выпускник должен обладать профессиональными компетенциями, соответствующими видам деятельности (обязательные результаты):		
Вид деятельности/трудо-вая функция	Наименование профессиональных компетенций (ФГОС ВО)	Шифр и название компетенции в ППП, для формирования трудовых функций, определенных профстандартом
А/01.5	ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-2 Способен применять информационно-коммуникационные технологии,	ОПК-ИБ-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах ОПК-ИБ-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях ОПК-ИБ-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-ИБ-2 Способен применять информационно-коммуникационные технологии,

	программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-ИБ-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-ИБ-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-ИБ-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности ОПК-ИБ-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК-ИБ-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-ИБ-11 Способен проводить эксперименты по заданной методике и обработку их результатов
A/02.5	ОПК-1.2 Способен администрировать средства	ОПК-ИБ-1.2 Способен администрировать средства

	защиты информации в компьютерных системах и сетях ОПК-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК-10 Способен в качестве	защиты информации в компьютерных системах и сетях ОПК-ИБ-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям ОПК-ИБ-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-ИБ-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-ИБ-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности ОПК-ИБ-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности ОПК-ИБ-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-ИБ-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-ИБ-9 Способен применять средства криптографической и технической защиты информации для решения задач
--	--	--

	технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	профессиональной деятельности ОПК-ИБ-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-ИБ-11 Способен проводить эксперименты по заданной методике и обработку их результатов ОПК-ИБ-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
A/03.5	ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач	ОПК-ИБ-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства ОПК-ИБ-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах ОПК-ИБ-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях ОПК-ИБ-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-ИБ-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач

профессиональной деятельности ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов ОПК-12 Способен проводить	профессиональной деятельности ОПК-ИБ-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ОПК-ИБ-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-ИБ-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности ОПК-ИБ-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности ОПК-ИБ-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК-ИБ-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ОПК-ИБ-11 Способен проводить эксперименты по заданной методике и обработку их результатов ОПК-ИБ-12 Способен проводить
---	---

	подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
--	---	---

Выпускник, освоивший программу, способен к выполнению трудовых функций и необходимых для этого трудовых действий.

КАРТА КОМПЕТЕНЦИЙ

Карта компетенций программы профессиональной переподготовки представляет декомпозицию вышеуказанных компетенций на уровне «знать, уметь».

Соотнесение трудовых функций, трудовых действий, умений и навыков профессионального стандарта с формируемыми компетенциями

Трудовые функции	Трудовые действия	Умения	Знания	Шифр компетенции ДПП
А/01.5	- Ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах - Установка программно-аппаратных средств защиты информации - Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам - Установка средств антивирусной защиты в соответствии с действующими требованиями - Инструктирование пользователей по порядку безопасной работы в операционных системах - Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах - Восстановление работоспособности программно-аппаратных средств защиты информации в операционных	- Настраивать компоненты подсистем защиты информации операционных систем - Управлять учетными записями пользователей, в том числе генерированием, сменой и восстановлением паролей - Применять программно-аппаратные средства защиты информации в операционных системах - Применять антивирусные средства защиты информации в операционных системах - Работать в операционных системах с соблюдением действующих требований по защите информации - Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации - Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации - Контролировать целостность	- Архитектура и пользовательские интерфейсы операционных систем - Порядок обеспечения безопасности информации при эксплуатации операционных систем - Источники угроз информационной безопасности и меры по их предотвращению - Сущность и содержание понятия информационной безопасности, характеристики ее составляющих - Типовые средства защиты информации в операционных системах - Программно-аппаратные средства и методы защиты информации - Порядок эксплуатации средств антивирусной защиты в операционных системах - Формы и методы инструктирования пользователей по порядку работы в операционных системах - Общие принципы функционирования программно-аппаратных средств криптографической защиты информации - Порядок оформления эксплуатационной документации - Нормативные правовые акты в области защиты информации	ОПК-ИБ-1.1, ОПК-ИБ-1.2, ОПК-ИБ-1.4, ОПК-ИБ-2, ОПК-ИБ-5, ОПК-ИБ-6, ОПК-ИБ-8, ОПК-ИБ-9, ОПК-ИБ-10, ОПК-ИБ-11

	системах согласно технической документации • Проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением	подсистем защиты информации операционных систем • Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации • Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации	• Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры • Организационные меры по защите информации	
A/02.5.	• Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях • Установка программно-аппаратных средств защиты информации в компьютерных сетях • Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации • Настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам • Устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации • Инструктирование пользователей по порядку безопасной работы в компьютерных сетях • Оформление эксплуатационной документации на программно-аппаратные средства защиты	• Применять программно-аппаратные средства защиты информации в компьютерных сетях • Устанавливать межсетевые экраны в компьютерных сетях • Конфигурировать межсетевые экраны в соответствии с заданными правилами • Контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами • Работать в компьютерных сетях с соблюдением действующих требований по защите информации • Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях • Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации • Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях	• Топология и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях • Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей • Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях • Типичные сетевые атаки и способы защиты от них • Сущность и содержание понятия информационной безопасности, характеристики ее составляющих • Основные источники угроз информационной безопасности и меры по их предотвращению • Программно-аппаратные средства и методы защиты информации • Основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей • Порядок оформления эксплуатационной документации • Общие принципы функционирования средств криптографической защиты	ОПК-ИБ-1.2, ОПК-ИБ-1.3, ОПК-ИБ-1.4, ОПК-ИБ-2, ОПК-ИБ-3, ОПК-ИБ-4, ОПК-ИБ-5, ОПК-ИБ-6, ОПК-ИБ-9, ОПК-ИБ-10, ОПК-ИБ-11, ОПК-ИБ-12

	информации в компьютерных сетях		информации в компьютерных сетях • Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей • Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях • Нормативные правовые акты в области защиты информации • Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры • Организационные меры по защите информации	
A/03.5	• Установка программного обеспечения • Настройка программного обеспечения с соблюдением требований по защите информации • Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам • Инструктирование пользователей о соблюдении требований по защите информации при работе с программным обеспечением • Настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам • Проверка функционирования	• Устанавливать программное обеспечение в соответствии с технической документацией • Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота • Работать с программным обеспечением с соблюдением действующих требований по защите информации • Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации	• Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота • Общие принципы функционирования вредоносного программного обеспечения • Принципы функционирования средств антивирусной защиты • Сущность и содержание понятия информационной безопасности, характеристики ее составляющих • Источники угроз информационной безопасности и меры по их предотвращению • Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения • Признаки наличия вредоносного программного обеспечения	ОПК-ИБ-1, ОПК-ИБ-1.1, ОПК-ИБ-1.2, ОПК-ИБ-1.4, ОПК-ИБ-2, ОПК-ИБ-5, ОПК-ИБ-6, ОПК-ИБ-7, ОПК-ИБ-8, ОПК-ИБ-9, ОПК-ИБ-10, ОПК-ИБ-11, ОПК-ИБ-12

	встроенных средств защиты информации программного обеспечения • Обнаружение признаков наличия вредоносного программного обеспечения		• Типичные уязвимости программного обеспечения и методы их устранения • Общие принципы функционирования средств защиты информации программного обеспечения, в том числе средств криптографической защиты информации • Порядок эксплуатации средств антивирусной защиты • Порядок обеспечения безопасности информации при эксплуатации программного обеспечения • Нормативные правовые акты в области защиты информации • Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры • Организационные меры по защите информации	
--	--	--	---	--

МАТРИЦА КОМПЕТЕНЦИЙ

Матрица компетенций с указанием оценочных средств

	Дисциплина	ОПК-ИБ-1	ОПК-ИБ-1.1	ОПК-ИБ-1.2	ОПК-ИБ-1.3	ОПК-ИБ-1.4	ОПК-ИБ-2	ОПК-ИБ-3	ОПК-ИБ-4	ОПК-ИБ-5	ОПК-ИБ-6	ОПК-ИБ-7	ОПК-ИБ-8	ОПК-ИБ-9	ОПК-ИБ-10	ОПК-ИБ-11	ОПК-ИБ-12	Форма аттестации	Результат
1.	Прикладной русский язык и деловые коммуникации												+					Зачет	Тест
2.	Цифровая трансформация	+					+											Зачет	Тест
3.	Безопасность сетей передачи данных				+	+												Зачет	Тест
4.	Криптографические средства защиты информации				+									+				Зачет	Тест
5.	Безопасность облачных сервисов			+		+												Зачет	Тест
6.	Вирусология			+												+		Зачет	Тест
7.	Объектно-ориентированные языки программирования и паттерны разработки			+								+						Зачет	Тест
8.	Компьютерные сети				+		+											Зачет	Тест
9.	Инструментальные средства разработки программного обеспечения											+				+		Зачет	Тест
10.	Прикладная математика							+								+		Зачет	Тест
11.	Экономика и управление														+		+	Зачет	Тест
12.	Основы алгоритмизации и программирования							+				+						Зачет	Тест
13.	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении			+							+							Зачет	Тест
14.	Сети и системы передачи информации				+				+									Зачет	Тест
15.	Электроника и схемотехника								+					+				Зачет	Тест
16.	Организационно-правовое обеспечение информационной безопасности									+	+							Зачет	Тест
17.	Защита информации в автоматизированных системах программными и программно-аппаратными средствами		+											+				Зачет	Тест

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

	Дисциплина	Форма контроля		Всего ак. часов	В том числе	
		Экзамен	Зачет		Самостоятельная работа	Лекции
1.	Прикладной русский язык и деловые коммуникации	0	Зачет	72	52	20
2.	Цифровая трансформация	0	Зачет	72	52	20
3.	Безопасность сетей передачи данных	0	Зачет	34	26	8
4.	Криптографические средства защиты информации	0	Зачет	34	26	8
5.	Безопасность облачных сервисов	0	Зачет	34	26	8
6.	Вирусология	0	Зачет	34	26	8
7.	Объектно-ориентированные языки программирования и паттерны разработки	0	Зачет	34	26	8
8.	Компьютерные сети	0	Зачет	34	26	8
9.	Инструментальные средства разработки программного обеспечения	0	Зачет	34	26	8
10.	Прикладная математика	0	Зачет	144	116	28
11.	Экономика и управление	0	Зачет	72	52	20
12.	Основы алгоритмизации и программирования	0	Зачет	144	116	28
13.	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	0	Зачет	72	52	20
14.	Сети и системы передачи информации	0	Зачет	72	52	20
15.	Электроника и схемотехника	0	Зачет	108	86	22
16.	Организационно-правовое обеспечение информационной безопасности	0	Зачет	108	86	22
17.	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	0	Зачет	180	144	36
18.	Итоговая аттестация	Тестирование	0	0	0	4
	ИТОГО:	0	0	1286	990	296

2.2. Сводные данные по бюджету времени

Продолжительность обучения	Теоретическое обучение	Практические занятия	Промежуточная аттестация	Итоговая аттестация
Всего (час.)				
1 год	1027	2	Зачет	-
2 год	259	2	Зачет	Тестирование
ИТОГО:	1282	4	-	1286

3. РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН, ПРАКТИКИ

Рабочая программа дисциплины «Прикладной русский язык и деловые коммуникации»

Рабочая программа дисциплины «Цифровая трансформация»

Рабочая программа дисциплины «Безопасность сетей передачи данных»

Рабочая программа дисциплины «Криптографические средства защиты информации»

Рабочая программа дисциплины «Безопасность облачных сервисов»

Рабочая программа дисциплины «Вирусология»

Рабочая программа дисциплины «Объектно-ориентированные языки программирования и паттерны разработки»

Рабочая программа дисциплины «Компьютерные сети»

Рабочая программа дисциплины «Инструментальные средства разработки программного обеспечения»

Рабочая программа дисциплины «Прикладная математика»

Рабочая программа дисциплины «Экономика и управление»

Рабочая программа дисциплины «Основы алгоритмизации и программирования»

Рабочая программа дисциплины «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

Рабочая программа дисциплины «Сети и системы передачи информации»

Рабочая программа дисциплины «Электроника и схемотехника»

Рабочая программа дисциплины «Организационно-правовое обеспечение информационной безопасности»

Рабочая программа дисциплины «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

3.1 Формы аттестации, оценочные материалы и критерии оценивания результатов обучения

Итоговая аттестация предполагает проверку результатов освоения программы профессиональной переподготовки, т.е. оценку сформированных всех компетенций, предусмотренных программой.

Аттестация осуществляется в форме просмотра сформированного индивидуального портфолио и/или тестирования.

Предмет и объект оценивания с указанием критериев и шкал

Предмет оценивания знания, умения, владение	Объект оценивания - продукт деятельности процесс, продукт и процесс	Показатели оценки	Критерии оценки	Шкалы оценки
Знания Присвоенные ОПК-ИБ-1 ОПК-ИБ-1.1 ОПК-ИБ-1.2 ОПК-ИБ-1.3 ОПК-ИБ-1.4 ОПК-ИБ-2 ОПК-ИБ-3 ОПК-ИБ-4 ОПК-ИБ-5 ОПК-ИБ-6 ОПК-ИБ-7 ОПК-ИБ-8 ОПК-ИБ-9 ОПК-ИБ-10 ОПК-ИБ-11 ОПК-ИБ-12	Ответ на вопросы членов комиссии или отсутствие ответов	Актуальность Научность Полнота изложения	Слушатель способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих и конкретных задач	Отлично Компетенции освоены в полном объеме (100 - 90%)
			Слушатель способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Хорошо Компетенции освоены от 66% до 89%
			Слушатель способен применять знания в ограниченной области профессиональной деятельности	Удовлетворительно Компетенции освоены от 50% до 65%
			Слушатель не способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Неудовлетворительно Компетенции освоены меньше 50%
			Слушатель способен применять знания в широкой и ограниченной области профессиональной деятельности при решении теоретических и	Зачтено Компетенции освоены от 50% и более

			практических задач	
			Слушатель не способен применять знания в широкой области профессиональной деятельности при решении общих и конкретных задач	Не зачтено Компетенции освоены меньше 50%
Умения ОПК-ИБ-1 ОПК-ИБ-1.1 ОПК-ИБ-1.2 ОПК-ИБ-1.3 ОПК-ИБ-1.4 ОПК-ИБ-2 ОПК-ИБ-3 ОПК-ИБ-4 ОПК-ИБ-5 ОПК-ИБ-6 ОПК-ИБ-7 ОПК-ИБ-8 ОПК-ИБ-9 ОПК-ИБ-10 ОПК-ИБ-11 ОПК-ИБ-12	Выполнение практических заданий в период подготовки к итоговой защите работы	Достижение планового результата Активность, инициатива, толерантность, лидерство Качество и полнота аргументов, умение отстоять свою точку зрения	Слушатель способен применять умения в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих и конкретных задач	Отлично Компетенции освоены в полном объеме (100 - 90%)
			Слушатель способен применять умения в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Хорошо Компетенции освоены от 66% до 89%
			Слушатель способен применять умения в ограниченной области профессиональной деятельности	Удовлетворительно Компетенции освоены от 50% до 65%
			Слушатель не способен применять умения в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Неудовлетворительно Компетенции освоены меньше 50%
			Слушатель способен применять умения в широкой и ограниченной области профессиональной деятельности при решении теоретических и практических задач	Зачтено Компетенции освоены от 50% и более
			Слушатель не способен применять умения в широкой области профессиональной деятельности при решении общих и конкретных задач	Не зачтено Компетенции освоены меньше 50%
Навыки (опыт деятельности) ОПК-ИБ-1 ОПК-ИБ-1.1 ОПК-ИБ-1.2	Использование полученных знаний в практической деятельности на	Достижение поставленной цели в практической деятельности на	Слушатель способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе	Отлично Компетенции освоены в полном объеме (100 - 90%)

ОПК-ИБ-1.3 ОПК-ИБ-1.4 ОПК-ИБ-2 ОПК-ИБ-3 ОПК-ИБ-4 ОПК-ИБ-5 ОПК-ИБ-6 ОПК-ИБ-7 ОПК-ИБ-8 ОПК-ИБ-9 ОПК-ИБ-10 ОПК-ИБ-11 ОПК-ИБ-12	предприятия в период стажировки и подготовки к итоговой защите работы	предприятия (в организации) - самооценка	приобретенного практического опыта при решении общих и конкретных задач	
			Слушатель способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Хорошо Компетенции освоены от 66% до 89%
			Слушатель способен применять знания в ограниченной области профессиональной деятельности	Удовлетворительно Компетенции освоены от 50% до 65%
			Слушатель не способен применять знания в широкой области профессиональной деятельности, успешно действовать на основе приобретенного практического опыта при решении общих задач	Неудовлетворительно Компетенции освоены меньше 50%
			Слушатель способен применять знания в широкой и ограниченной области профессиональной деятельности при решении теоретических и практических задач	Зачтено Компетенции освоены от 50% и более
			Слушатель не способен применять знания в широкой области профессиональной деятельности при решении общих и конкретных задач	Не зачтено Компетенции освоены меньше 50%

Оценочные материалы, методические указания и другая информация, касающаяся оценки результатов освоения программы приводится в программе итоговой аттестации.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Реализация дополнительной профессиональной программы (профессиональной переподготовки) осуществляется в соответствии с требованиями российского законодательства, нормативными актами Министерства науки и высшего образования РФ, уставом АНО ВО «Университет ИТ ХАБ», лицензией №Л035-00115-77/02130099 от 15 апреля 2025г. на осуществление образовательной деятельности. (размещена на сайте образовательной организации <https://univer.ithub.ru/sveden/>).

4.1 Требования к квалификации педагогических кадров

Реализация программы профессиональной переподготовки обеспечивается руководящими и научно-педагогическими работниками организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Требования к квалификации педагогических кадров, обеспечивающих реализацию образовательного процесса, формулируются согласно Приказа Минтруда России от 26.12.2019 N 832н "Об утверждении профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования" (Зарегистрировано в Минюсте России 01.06.2020 N 58533) - «Преподавание по программам профессионального обучения, среднего профессионального образования (СПО) и дополнительным профессиональным программам (ДПП), ориентированным на соответствующий уровень квалификации» (А 6).

4.2. Материально-технические условия реализации программы

Технические средства обучения

Для реализации программы используется собственная материально-техническая база. Для реализации программы предполагается использование имеющихся в АНО ВО «Университет ИТ ХАБ» учебных аудиторий для проведения занятий лекционного типа, занятий семинарского типа, выполнения проектных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования:

- компьютерные классы, обеспечивающие доступ в Интернет, с установленным лицензионными программами, необходимыми для изучения дисциплин/курсов программы, оснащенные проектором или иными средствами визуализации учебного материала.

- доступ в электронную информационно-образовательную среду АНО ВО «Университет ИТ ХАБ»;

- стандартное программное обеспечение для работы над разработкой учебно-методических материалов.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

4.3. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

4.4. Общие требования к организации образовательного процесса

Обучение предполагает взаимодействие с применением современных дистанционных образовательных технологий.

Формы занятий включают как теоретическую часть (направленную на получение или пополнение имеющихся знаний), так и практическую, имеющую преимущественно общепрофессиональную направленность. На формирование практико-ориентированных компетенций слушателей направлено активное использование в учебном процессе инновационных образовательных технологий.

В процессе освоения дополнительной профессиональной программы, обучающиеся формируют портфолио по результатам освоения учебных модулей.

Итоговая аттестация предполагает определение уровня сформированных компетенций на основе оценки портфолио или проекта (результат деятельности) и приобретенных знаний (может осуществляться как в устной форме, так и в форме итогового тестирования).

Образовательная деятельность слушателей предусматривает следующие виды учебных работ: лекции, практические занятия, консультации и другие виды учебных занятий и методической работы, определенные учебным планом.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Прикладной русский язык и деловые коммуникации

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ
ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 72 часов

Виды занятий	Объем часов
Лекции	20 часов
Самостоятельная работа	52 часа
Аттестация	Зачет
ВСЕГО:	72 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания теоретических и концептуальных представлений о нормах

современного русского языка, стилистике профессиональной речи и принципах делового общения, а также практических навыков и умений, позволяющих им в будущем осуществлять грамотное документирование сетевых инфраструктур, вести профессиональную переписку и аргументированно представлять решения в сфере информационной безопасности в условиях междисциплинарного взаимодействия и работы с техническими заказчиками.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-ИБ-8

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост оятель ная работа	
1	Тема 1. Русский язык. Коммуникативные практики. Цифровой этикет и язык интернета	36	36	10	26	-
2	Тема 2. Цифровой этикет	36	36	10	26	-
	ВСЕГО	72	72	20	52	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Русский язык. Коммуникативные практики. Цифровой этикет и язык интернета

- Язык интернета
- Особенности пунктуации в интернете
- Анализ пробоев и стратегии аргументации
- Аргументация и импровизация

Тема 2. Цифровой этикет

- Проблемы чатов и соцсетей
- Правила для комфортного общения
- Командная работа и практика коммуникации

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения. Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Русский язык. Коммуникативные практики. Цифровой этикет и язык интернета	Тестирование
2	Тема 2. Цифровой этикет	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Как в современной цифровой переписке (мессенджеры) чаще всего воспринимается одиночная точка в конце короткого сообщения (например, «Хорошо.»)?

- А) Как признак высокой грамматической грамотности отправителя
- Б) Как пассивная агрессия, холодность или скрытое недовольство
- В) Как срочность и критическая важность передаваемой информации
- Г) Как случайная опечатка, на которую не стоит обращать внимания

Вопрос 2 Что такое «анализ пробелом» (или создание «воздуха в тексте») в деловой цифровой коммуникации?

- А) Использование невидимых символов для скрытия конфиденциальной информации
- Б) Разделение текста на короткие абзацы с пустыми строками между ними для облегчения чтения с экрана
- В) Написание сообщения заглавными буквами для привлечения внимания
- Г) Удаление всех знаков препинания для ускорения набора текста

Вопрос 3 Какой прием аргументации предполагает предварительное согласие с доводами оппонента перед выдвижением контраргументов, чтобы снизить конфликтность и повысить доверие?

- А) Метод «Сэндвича»
- Б) Техника «Да, но...» (или «Присоединение»)
- В) Метод «Адвоката дьявола»
- Г) Тактика «Выжженной земли»

Вопрос 4 Для чего в деловых коммуникациях и импровизированных выступлениях используется структура PREP (Point, Reason, Example, Point)?

- А) Для шифрования конфиденциальных данных в отчете
- Б) Для быстрого и структурированного формулирования убедительной мысли или ответа на вопрос
- В) Для оценки эффективности командной работы по итогам квартала
- Г) Для автоматического перевода текста на иностранный язык

Вопрос 5 Каково рекомендуемое правило использования эмодзи и стикеров в официальной деловой переписке с клиентами или руководством?

- А) Обязательно использовать в каждом сообщении для поддержания дружелюбного тона
- Б) Использовать только в конце предложения вместо точки
- В) Избегать или использовать крайне осторожно и уместно, так как они могут снизить статусность и быть неправильно истолкованы
- Г) Заменять эмодзи все числительные и даты для экономии символов

Вопрос 6 Согласно правилам цифрового этикета, каков главный принцип отправки голосовых сообщений (войсов) в рабочие чаты?

- А) Голосовые сообщения следует отправлять только в экстренных случаях, когда нет возможности печатать

- Б) Отправлять голосовые сообщения можно только после получения явного согласия собеседника или если это заранее оговорено в команде
- В) Голосовые сообщения запрещены во всех корпоративных мессенджерах
- Г) Голосовые сообщения предпочтительнее текстовых, так как они передают больше эмоций

Вопрос 7 Как правильно привлечь внимание конкретного коллеги в общем рабочем чате, чтобы не уведомлять всех его участников?

- А) Написать его имя заглавными буквами (CAPS LOCK)
- Б) Использовать функцию упоминания (тегирование через @)
- В) Отправить личное сообщение с просьбой прочитать общий чат
- Г) Начать сообщение со слов «Внимание всем, это касается только Ивана»

Вопрос 8 Какое базовое правило цифрового этикета необходимо соблюдать при участии в командных онлайн-встречах (Zoom, Teams, Яндекс.Телемост)?

- А) Держать микрофон включенным, чтобы коллеги слышали фоновый шум и понимали, что вы на связи
- Б) Отключать микрофон, когда вы не говорите, и включать камеру, если это предусмотрено форматом встречи
- В) Параллельно работать с документами, не включая камеру и микрофон, чтобы не отвлекать спикера
- Г) Использовать виртуальный фон только в том случае, если вы опоздали на встречу

Вопрос 9 Что подразумевает соблюдение «границ рабочего времени» в цифровой среде?

- А) Возможность отправлять рабочие сообщения в любое время, так как получатель сам решит, когда их прочитать
- Б) Запрет на использование корпоративных мессенджеров в выходные и нерабочее время, кроме случаев форс-мажора
- В) Обязательство отвечать на все рабочие чаты мгновенно, даже в ночное время
- Г) Автоматическое отключение серверов компании в 18:00

Вопрос 10 Что из перечисленного является нарушением «информационной гигиены» в рабочем чате?

- А) Закрепление важных инструкций и регламентов в шапку чата
- Б) Ежедневная отправка открыток с пожеланиями «Доброго утра» и «Хорошего дня» в общий чат на 50 человек
- В) Использование веток (тредов) для обсуждения узких тем
- Г) Формулирование четкой темы перед отправкой файла или ссылки

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Цифровая трансформация

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 72 часов

Виды занятий	Объем часов
Лекции	20 часов
Самостоятельная работа	52 часа
Аттестация	Зачет
ВСЕГО:	72 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания сущности и направлений цифровой трансформации организаций, принципов платформенных бизнес-моделей и управления цифровой зрелостью, а также практических умений оценивать роль информации и цифровых технологий, выбирать и применять информационно-коммуникационные и программные средства для решения профессиональных задач с учетом требований информационной безопасности.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-ИБ-1
2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-ИБ-2

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-ИБ-1
2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-ИБ-2

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Цифровая трансформация и платформенные бизнес-модели	36	36	10	26	-
2	Тема 2. Управление цифровой зрелостью бизнеса	36	36	10	26	-
	ВСЕГО	72	72	20	52	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Цифровая трансформация и платформенные бизнес-модели

- Понятие, цели и ключевые направления цифровой трансформации организации
- Платформенные бизнес-модели, цифровые экосистемы и сетевые эффекты
- Данные, облачные технологии, интеграционные решения и цифровые сервисы как ресурсы трансформации
- Роль информационной безопасности и управления рисками в цифровой трансформации

Тема 2. Управление цифровой зрелостью бизнеса

- Понятие цифровой зрелости и основные направления ее оценки
- Модели, показатели и уровни цифровой зрелости организации
- Формирование дорожной карты цифрового развития и выбор цифровых решений
- Мониторинг результатов цифровой трансформации, управление изменениями и непрерывное совершенствование

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения. Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Цифровая трансформация и платформенные бизнес-модели	Тестирование
2	Тема 2. Управление цифровой зрелостью бизнеса	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что наиболее точно характеризует цифровую трансформацию организации?

- А) Только перевод бумажных документов в электронный вид
- Б) Системное изменение процессов, продуктов и моделей управления на основе цифровых технологий и данных
- В) Замена всех сотрудников программными роботами
- Г) Покупка нового компьютерного оборудования без изменения процессов

Вопрос 2 В чем ключевая особенность платформенной бизнес-модели?

- А) Создание условий для взаимодействия нескольких групп участников на единой цифровой платформе
- Б) Работа исключительно через физические точки продаж
- В) Отказ от использования данных о клиентах и операциях
- Г) Производство только одного стандартизированного продукта

Вопрос 3 Что означает сетевой эффект для цифровой платформы?

- А) Снижение качества сервиса по мере роста числа пользователей
- Б) Рост ценности платформы для участников по мере увеличения числа пользователей или партнеров
- В) Обязательное объединение всех информационных систем в одну локальную сеть
- Г) Переход организации на полностью автономную работу без внешних участников

Вопрос 4 Какую роль данные играют в цифровой трансформации?

- А) Используются только для архивного хранения отчетности
- Б) Являются ресурсом для анализа, принятия решений, автоматизации и создания новых сервисов
- В) Имеют значение только для бухгалтерского учета
- Г) Исключают необходимость управленческих решений

Вопрос 5 Почему информационная безопасность должна учитываться при цифровой трансформации?

- А) Потому что она относится только к работе системных администраторов
- Б) Потому что расширение цифровых процессов и обмена данными увеличивает требования к защите информации, устойчивости и управлению рисками
- В) Потому что она позволяет полностью отказаться от резервного копирования
- Г) Потому что она заменяет управление бизнес-процессами

Вопрос 6 Что понимается под цифровой зрелостью организации?

- А) Количество компьютеров на одного сотрудника
- Б) Степень развития способностей организации использовать данные, технологии, процессы и компетенции для достижения стратегических целей
- В) Возраст используемого программного обеспечения
- Г) Число зарегистрированных аккаунтов в корпоративных системах

Вопрос 7 Для чего организации оценивают цифровую зрелость?

- А) Чтобы определить текущее состояние, выявить разрывы и приоритеты цифрового развития
- Б) Чтобы отказаться от стратегического планирования
- В) Чтобы заменить все показатели эффективности одним техническим показателем
- Г) Чтобы оценить только скорость интернет-соединения

Вопрос 8 Что должно лежать в основе дорожной карты цифровой трансформации?

- А) Перечень модных технологий без связи с задачами организации
- Б) Стратегические цели, выявленные разрывы цифровой зрелости, приоритеты, ресурсы, риски и измеримые результаты
- В) Только календарь закупок оборудования
- Г) Только перечень программного обеспечения конкурентов

Вопрос 9 Какой подход наиболее обоснован при выборе программных средств для профессиональных задач?

- А) Выбирать решение только по известности бренда
- Б) Сопоставлять функциональные требования, совместимость, безопасность, стоимость владения и условия эксплуатации, включая доступные отечественные решения
- В) Всегда выбирать самое дорогое решение
- Г) Не учитывать интеграцию с существующей ИТ-инфраструктурой

Вопрос 10 Какой показатель лучше всего свидетельствует о результативности цифровой трансформации?

- А) Сам факт внедрения новой информационной системы
- Б) Достижение измеримых бизнес- и операционных эффектов: повышение качества, скорости, прозрачности процессов или ценности для пользователей
- В) Увеличение количества совещаний по цифровизации
- Г) Максимальное количество цифровых инициатив независимо от их результата

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность сетей передачи данных

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часов

Виды занятий	Объем часов
---------------------	--------------------

Лекции	8 часов
--------	---------

Самостоятельная работа	26 часов
------------------------	----------

Аттестация	Зачет
------------	-------

ВСЕГО:	34 часа
---------------	----------------

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов построения и защиты сетей передачи данных, угроз и уязвимостей сетевой инфраструктуры, а также практических навыков применения организационных и технических мер защиты информации при передаче по компьютерным сетям, контроля защищенности сетевых соединений и оценки уровня безопасности компьютерных систем и сетей в соответствии с нормативными и корпоративными требованиями.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-ИБ-1.4

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-ИБ-1.4

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Основы безопасности сетей передачи данных	12	12	3	9	-
2	Тема 2. Технологии защиты информации при передаче данных	11	11	3	8	-

3	Тема 3. Оценка защищенности и контроль безопасности компьютерных сетей	11	11	2	9	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Основы безопасности сетей передачи данных

- Архитектура сетей передачи данных и основные сетевые протоколы
- Классификация угроз и уязвимостей сетевой инфраструктуры
- Модель нарушителя и основные векторы сетевых атак
- Принципы сегментации сети и разграничения сетевого доступа

Тема 2. Технологии защиты информации при передаче данных

- Криптографическая защита передаваемой информации и защищенные протоколы
- Межсетевое экранирование, фильтрация трафика и системы предотвращения вторжений
- Виртуальные частные сети и организация защищенного удаленного доступа

Тема 3. Оценка защищенности и контроль безопасности компьютерных сетей

- Методы контроля защищенности и мониторинга сетевой инфраструктуры
- Оценка уровня безопасности компьютерных систем и сетей
- Анализ журналов событий, сетевого трафика и результатов сканирования уязвимостей
- Нормативные и корпоративные требования к защите сетей передачи данных

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>

Текущая аттестация:

Тестирование (выполнение заданий)

Наименование модулей по программе	Форма ТА
-----------------------------------	----------

1	Тема 1. Основы безопасности сетей передачи данных	Тестирование
2	Тема 2. Технологии защиты информации при передаче данных	Тестирование
3	Тема 3. Оценка защищенности и контроль безопасности компьютерных сетей	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какова основная цель сегментации компьютерной сети?

- А) Увеличение длины сетевых кабелей
- Б) Ограничение распространения сетевых угроз и разделение зон доступа
- В) Замена маршрутизаторов на коммутаторы
- Г) Полное отключение журналирования

Вопрос 2 Какое средство предназначено прежде всего для фильтрации сетевого трафика по заданным правилам?

- А) Межсетевой экран
- Б) Текстовый редактор
- В) Система резервного копирования
- Г) Система управления базами данных

Вопрос 3 Какой протокол обеспечивает защищенную передачу данных при доступе к веб-ресурсам?

- А) HTTP
- Б) FTP
- В) HTTPS
- Г) ARP

Вопрос 4 Для чего применяется VPN при организации удаленного доступа?

- А) Для формирования защищенного логического канала связи через общедоступную сеть
- Б) Для увеличения физической пропускной способности кабеля
- В) Для отключения аутентификации пользователей
- Г) Для замены антивирусной защиты

Вопрос 5 Что является одной из основных задач системы обнаружения или предотвращения вторжений?

- А) Выявление признаков сетевых атак и аномальной активности
- Б) Создание резервных копий бухгалтерских документов
- В) Форматирование дисков рабочих станций
- Г) Управление кадровым учетом

Вопрос 6 Какой принцип следует применять при предоставлении пользователям и сервисам сетевых прав доступа?

- А) Принцип максимальных привилегий
- Б) Принцип наименьших необходимых привилегий
- В) Принцип общего доступа без ограничений
- Г) Принцип отключения аутентификации

Вопрос 7 Что позволяет выявить сканирование уязвимостей сетевой инфраструктуры?

- А) Потенциальные слабые места и известные уязвимости узлов и сервисов
- Б) Только физические повреждения кабеля
- В) Только ошибки пользователей при наборе текста
- Г) Исключительно объем свободного места на диске

Вопрос 8 Какое действие наиболее уместно при обнаружении подозрительной сетевой активности?

- А) Игнорировать событие до появления сбоя
- Б) Зафиксировать событие, проанализировать журналы и трафик и действовать по процедуре реагирования
- В) Удалить все журналы событий
- Г) Отключить все средства защиты

Вопрос 9 Для чего проводится оценка уровня безопасности компьютерной сети?

- А) Для определения соответствия применяемых мер защиты выявленным рискам и установленным требованиям
- Б) Только для измерения скорости подключения к Интернету
- В) Для выбора дизайна корпоративного сайта
- Г) Для расчета количества сотрудников

Вопрос 10 Что должно учитываться при настройке средств защиты сетей передачи данных в организации?

- А) Только личные предпочтения администратора
- Б) Нормативные, корпоративные требования и результаты оценки рисков
- В) Только стоимость оборудования
- Г) Только количество рабочих станций

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические средства защиты информации

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часа

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов криптографической защиты информации и практических умений применять

криптографические средства для обеспечения конфиденциальности, целостности, аутентичности и защищенной передачи данных в компьютерных системах и сетях, а также безопасно использовать криптографические ключи и средства защиты при решении профессиональных задач в области информационной безопасности.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост оятель ная работа	
1	Тема 1. Основы криптографической защиты информации	12	12	3	9	-
2	Тема 2. Криптографические алгоритмы и управление ключевой информацией	11	11	3	8	-
3	Тема 3. Применение криптографических средств для защиты данных и сетевого взаимодействия	11	11	2	9	-

	ВСЕГО	34	34	8	26	
	Промежуточная аттестация					Тестирование

2. Рабочие программы учебных предметов

Тема 1. Основы криптографической защиты информации

- Назначение криптографической защиты информации и базовые криптографические понятия.
- Конфиденциальность, целостность, аутентичность и неотказуемость как задачи криптографической защиты.
- Симметричные и асимметричные криптосистемы: принципы действия, преимущества и ограничения.
- Криптографические хэш-функции и коды аутентификации сообщений.

Тема 2. Криптографические алгоритмы и управление ключевой информацией

- Принципы работы блочных и потоковых алгоритмов шифрования.
- Асимметричное шифрование, электронная подпись и инфраструктура открытых ключей.
- Генерация, распределение, хранение, ротация, резервирование и отзыв криптографических ключей.
- Требования к безопасной эксплуатации криптографических алгоритмов и средств защиты информации.

Тема 3. Применение криптографических средств для защиты данных и сетевого взаимодействия

- Криптографическая защита данных при хранении и работе с базами данных.
- Криптографическая защита информации при передаче по компьютерным сетям и организация защищенных каналов связи.
- Применение средств криптографической защиты информации в корпоративной информационной инфраструктуре.
- Контроль корректности настройки криптографических средств, управление сертификатами и предупреждение типовых ошибок эксплуатации.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиокolonками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Основы криптографической защиты информации	Тестирование
2	Тема 2. Криптографические алгоритмы и управление ключевой информацией	Тестирование
3	Тема 3. Применение криптографических средств для защиты данных и сетевого взаимодействия	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что является основной целью криптографического шифрования?

- А) Увеличение скорости передачи данных
- Б) Обеспечение конфиденциальности информации
- В) Сжатие информации
- Г) Удаление метаданных

Вопрос 2 Какой тип криптографии использует один и тот же секретный ключ для шифрования и расшифрования?

- А) Симметричная криптография
- Б) Асимметричная криптография
- В) Хэширование
- Г) Стеганография

Вопрос 3 Для чего применяется криптографическая хэш-функция?

- А) Для восстановления исходного сообщения по хэшу
- Б) Для проверки целостности данных
- В) Для увеличения размера файла
- Г) Для назначения сетевых адресов

Вопрос 4 Каково назначение электронной подписи?

- А) Только скрыть содержание сообщения
- Б) Подтвердить подлинность и целостность подписанных данных
- В) Сжать передаваемые данные

Г) Заменить резервное копирование

Вопрос 5 Что относится к управлению жизненным циклом криптографического ключа?

А) Только создание ключа

Б) Генерация, распределение, хранение, ротация и вывод ключа из эксплуатации

В) Только публикация ключа

Г) Только шифрование данных

Вопрос 6 Какой протокол применяется для криптографической защиты соединения между веб-клиентом и сервером?

А) TLS

Б) ARP

В) ICMP

Г) FTP без шифрования

Вопрос 7 Какой ключ в асимметричной криптосистеме предназначен для открытого распространения?

А) Закрытый ключ

Б) Сеансовый пароль

В) Открытый ключ

Г) Мастер-ключ

Вопрос 8 Какое требование является принципиальным при хранении закрытого криптографического ключа?

А) Свободный доступ всех пользователей

Б) Защита от несанкционированного доступа и копирования

В) Хранение исключительно в открытом виде

Г) Передача по незащищенной электронной почте

Вопрос 9 Какая мера повышает защищенность информации при передаче по компьютерной сети?

А) Использование защищенного протокола и актуальных криптографических механизмов

Б) Отключение проверки сертификатов

В) Использование одного пароля во всех системах

Г) Передача секретного ключа вместе с шифротекстом в открытом виде

Вопрос 10 Что необходимо сделать при подтвержденной компрометации криптографического ключа?

А) Продолжить его использование до плановой замены

Б) Вывести ключ из эксплуатации или отозвать его и заменить новым

В) Опубликовать ключ для всех пользователей

Г) Отключить журналирование событий

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность облачных сервисов

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часов

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов безопасного использования и администрирования облачных сервисов, моделей

распределения ответственности за информационную безопасность, методов управления доступом, защиты сетевой инфраструктуры и данных в облачной среде, а также практических умений применять средства защиты информации и оценивать уровень безопасности облачных ресурсов в соответствии с нормативными и корпоративными требованиями.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-ИБ-1.4

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-ИБ-1.4

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оатель- ная работа	
1	Тема 1. Введение в облачные технологии	17	17	4	13	-
2	Тема 2. Обзор сервисов Яндекс Cloud	17	17	4	13	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Введение в облачные технологии

- Понятие облачных вычислений и основные характеристики облачной среды
- Модели предоставления облачных сервисов: IaaS, PaaS, SaaS
- Модели развертывания облаков и особенности их применения
- Модель разделения ответственности за безопасность между облачным провайдером и заказчиком
- Основные угрозы и риски информационной безопасности в облачной среде
- Базовые меры защиты: управление идентификацией и доступом, защита сетевого взаимодействия, шифрование и журналирование событий

Тема 2. Обзор сервисов Яндекс Cloud

- Архитектура и базовые понятия Yandex Cloud: облака, каталоги и ресурсы
- Yandex Identity and Access Management (IAM): пользователи, сервисные аккаунты, роли и принцип минимальных привилегий
- Yandex Virtual Private Cloud: облачные сети, подсети и группы безопасности
- Yandex Object Storage: управление доступом к бакетам и объектам, предотвращение несанкционированного публичного доступа
- Yandex Key Management Service: применение ключей шифрования для защиты данных
- Контроль и оценка защищенности облачной конфигурации: журналирование событий, проверка настроек доступа и соответствия корпоративным требованиям

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Введение в облачные технологии	Тестирование
2	Тема 2. Обзор сервисов Яндекс Cloud	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что наиболее точно характеризует модель IaaS?

- А) Пользователь получает только готовое прикладное приложение
- Б) Пользователь получает вычислительные, сетевые и дисковые ресурсы и самостоятельно управляет ОС и приложениями
- В) Пользователь арендует исключительно физическое помещение для серверов
- Г) Провайдер передает пользователю полный контроль над своей облачной инфраструктурой

Вопрос 2 Какой принцип следует применять при назначении прав доступа к облачным ресурсам?

- А) Выдавать всем пользователям права администратора для упрощения работы
- Б) Назначать минимально необходимые права для выполнения конкретных задач
- В) Использовать одну общую учетную запись для всех сотрудников
- Г) Отключать аутентификацию для внутренних сервисов

Вопрос 3 Что означает модель разделения ответственности в облачной среде?

- А) За все аспекты безопасности отвечает только облачный провайдер
- Б) За все аспекты безопасности отвечает только заказчик
- В) Обязанности по защите распределяются между провайдером и заказчиком в зависимости от используемой модели сервиса
- Г) Ответственность определяется только стоимостью облачного тарифа

Вопрос 4 Какое назначение имеет Yandex Identity and Access Management (IAM)?

- А) Централизованное управление идентификацией пользователей и правами доступа к облачным ресурсам
- Б) Создание резервных копий виртуальных машин
- В) Мониторинг температуры серверного оборудования
- Г) Автоматическое масштабирование приложений

Вопрос 5 Для чего в Yandex Virtual Private Cloud используются группы безопасности?

- А) Для управления сетевым трафиком к ресурсам с помощью разрешающих правил
- Б) Для создания учетных записей пользователей
- В) Для шифрования файлов в Object Storage
- Г) Для выставления счетов за потребленные ресурсы

Вопрос 6 Какой риск возникает при разрешении публичного доступа к бакету Object Storage без необходимости?

- А) Увеличение производительности сети
- Б) Возможность несанкционированного доступа к размещенным данным
- В) Автоматическое шифрование всех объектов
- Г) Блокирование работы IAM

Вопрос 7 Какое средство Yandex Cloud предназначено для централизованного управления ключами шифрования?

- А) Yandex Key Management Service
- Б) Yandex Virtual Private Cloud
- В) Yandex Object Storage
- Г) Yandex Compute Cloud

Вопрос 8 Что следует проверять при оценке безопасности облачной конфигурации?

- А) Только удобство интерфейса управления
- Б) Настройки доступа, сетевые правила, защиту данных и соответствие установленным требованиям
- В) Только количество созданных виртуальных машин

Г) Только стоимость используемых сервисов

Вопрос 9 Какой подход лучше всего снижает риск компрометации учетных данных сервисов?

- А) Использование постоянных ключей без ротации
- Б) Хранение ключей в открытом виде в исходном коде
- В) Применение ограниченных по правам учетных данных и безопасное управление секретами
- Г) Передача одной пары ключей всем участникам команды

Вопрос 10 Какое действие наиболее соответствует безопасной эксплуатации облачных сервисов?

- А) Регулярный анализ журналов событий и проверка изменений конфигурации
- Б) Отключение журналирования для экономии ресурсов
- В) Предоставление публичного доступа ко всем сервисам по умолчанию
- Г) Отказ от пересмотра прав доступа после изменения обязанностей сотрудников

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Вирусология

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часа

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: формирование у обучающихся системного представления о компьютерных вирусах и других видах вредоносного программного обеспечения, методах их выявления и безопасного исследования, а также практических умений по администрированию средств антивирусной защиты, проведению экспериментов по

заданной методике и обработке результатов для оценки эффективности применяемых средств защиты информации в компьютерных системах и сетях.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оятель- ная работа	
1	Тема 1. Основы компьютерной вирусологии и классификация вредоносного программного обеспечения	12	12	3	9	-
2	Тема 2. Методы обнаружения, анализа и исследования вредоносного программного обеспечения	11	11	3	8	-
3	Тема 3. Средства антивирусной защиты и экспериментальная оценка их эффективности	11	11	2	9	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Основы компьютерной вирусологии и классификация вредоносного программного обеспечения

- Понятие компьютерного вируса и вредоносного программного обеспечения; основные признаки и жизненный цикл вредоносного кода.
- Классификация вредоносного ПО: вирусы, черви, троянские программы, программы-вымогатели, шпионское ПО и иные типы угроз.
- Каналы распространения, факторы риска и базовые меры профилактики заражения компьютерных систем и сетей.

Тема 2. Методы обнаружения, анализа и исследования вредоносного программного обеспечения

- Сигнатурные, эвристические и поведенческие методы обнаружения вредоносной активности.
- Безопасные принципы статического и динамического анализа подозрительных объектов в изолированной среде.
- Постановка эксперимента по заданной методике, фиксация наблюдений, обработка и интерпретация результатов исследования.

Тема 3. Средства антивирусной защиты и экспериментальная оценка их эффективности

- Назначение, состав и принципы функционирования средств антивирусной защиты; обновление баз, карантин и контроль событий безопасности.
- Администрирование средств защиты информации: настройка политик, расписаний проверок, журналирования и реагирования на обнаружения.
- Экспериментальная оценка эффективности антивирусной защиты: выбор показателей, сопоставление результатов и формулирование выводов.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Основы компьютерной вирусологии и классификация	Тестирование

	вредоносного программного обеспечения	
2	Тема 2. Методы обнаружения, анализа и исследования вредоносного программного обеспечения	Тестирование
3	Тема 3. Средства антивирусной защиты и экспериментальная оценка их эффективности	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что наиболее точно характеризует компьютерный вирус?

- А) Вредоносный код, способный внедряться в другие объекты и распространять свои копии
- Б) Программа для резервного копирования данных
- В) Любая программа, работающая без подключения к Интернету
- Г) Системная служба операционной системы

Вопрос 2 Какой тип вредоносного ПО обычно способен самостоятельно распространяться по сети без внедрения в другой файл?

- А) Сетевой червь
- Б) Архиватор
- В) Драйвер устройства
- Г) Текстовый редактор

Вопрос 3 Какова основная задача сигнатурного метода обнаружения вредоносного ПО?

- А) Сравнение объекта с известными характерными признаками вредоносного кода
- Б) Увеличение скорости сетевого соединения
- В) Шифрование всех пользовательских файлов
- Г) Создание резервных копий системы

Вопрос 4 Для чего при исследовании подозрительного файла используется изолированная среда (песочница)?

- А) Для безопасного наблюдения за поведением объекта с ограничением его воздействия на рабочую среду
- Б) Для ускорения работы офисных приложений
- В) Для отключения журналирования событий
- Г) Для хранения паролей пользователей

Вопрос 5 Что относится к результатам динамического анализа подозрительного программного объекта?

- А) Наблюдение за процессами, сетевой активностью и изменениями системы во время выполнения объекта
- Б) Только чтение названия файла
- В) Определение размера экрана компьютера
- Г) Проверка орфографии в документах

Вопрос 6 Какое действие наиболее соответствует администрированию средств антивирусной защиты?

- А) Настройка политик проверки, обновлений, карантина и журналирования событий
- Б) Замена сетевых кабелей по расписанию
- В) Подготовка презентаций для сотрудников
- Г) Изменение формата офисных документов

Вопрос 7 Для чего регулярно обновляются антивирусные базы и механизмы обнаружения?

- А) Для распознавания новых и измененных угроз

- Б) Для увеличения объема оперативной памяти
- В) Для изменения IP-адреса компьютера
- Г) Для ускорения печати документов

Вопрос 8 Что необходимо обеспечить при проведении эксперимента по заданной методике?

- А) Воспроизводимость условий, фиксацию параметров и результатов
- Б) Изменение условий на каждом шаге без документирования
- В) Отказ от измеримых показателей
- Г) Использование только субъективной оценки

Вопрос 9 Какой показатель может использоваться при экспериментальной оценке эффективности средства антивирусной защиты?

- А) Доля корректно обнаруженных тестовых угроз при заданных условиях проверки
- Б) Количество символов в имени компьютера
- В) Размер рабочего стола пользователя
- Г) Число открытых вкладок браузера

Вопрос 10 Что означает ложное срабатывание средства защиты?

- А) Безопасный объект ошибочно классифицирован как вредоносный
- Б) Вредоносный объект корректно обнаружен
- В) Обновление антивирусной базы завершено успешно
- Г) Пользователь выполнил резервное копирование

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Объектно-ориентированные языки программирования и паттерны разработки

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часа

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов объектно-ориентированного программирования и практических навыков разработки программных средств на языке Python с использованием модулей, итераторов, генераторов, потоковой обработки больших файлов и фильтрации данных, а также

применение указанных средств при автоматизации задач администрирования и защиты информации в компьютерных системах и сетях.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-ИБ-7

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Администрировать и применять программные средства и сценарии автоматизации для поддержки задач защиты информации в компьютерных системах и сетях, соблюдая требования безопасной обработки данных.	ОПК-ИБ-1.2
2	Использовать объектно-ориентированный подход, модули, итераторы, генераторы, средства чтения больших файлов и фильтрации данных языка Python для разработки программных решений профессиональных задач.	ОПК-ИБ-7

1. Учебный план:

№	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	Лекции	Самостоятельная работа	Форма ТА
1	Тема 1. Модули	9	9	2	7	-
2	Тема 2. Итераторы и генераторы	9	9	2	7	-
3	Тема 3. Чтение больших файлов	8	8	2	6	-
4	Тема 4. Фильтры	8	8	2	6	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Модули

Понятие модуля и пакета. Организация программного кода и пространства имен.

Импорт модулей, относительный и абсолютный импорт. Повторное использование компонентов.

Разработка собственных модулей и структура проекта. Инкапсуляция функциональности.

Применение модульного подхода при создании средств автоматизации задач администрирования и информационной безопасности.

Тема 2. Итераторы и генераторы

Итерируемые объекты и протокол итерации. Функции `iter()` и `next()`.

Создание пользовательских итераторов. Принципы ленивых вычислений.

Генераторные функции и выражения, оператор `yield`. Управление памятью при обработке последовательностей.

Использование итераторов и генераторов для обработки журналов событий и потоков данных.

Тема 3. Чтение больших файлов

Работа с файловыми объектами и контекстными менеджерами. Режимы открытия файлов.

Построчное и блочное чтение больших файлов без полной загрузки в оперативную память.

Обработка кодировок, исключений и некорректных данных. Безопасная работа с путями и файлами.

Потоковый анализ журналов, отчетов и иных массивов данных, используемых при администрировании средств защиты информации.

Тема 4. Фильтры

Фильтрация последовательностей с помощью условных выражений, списковых включений и функции `filter()`.

Применение `lambda`-функций и именованных предикатов. Сочетание фильтрации с итераторами и генераторами.

Построение конвейеров отбора, преобразования и анализа данных.

Фильтрация событий безопасности, записей журналов и технических данных по заданным критериям.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Модули	Тестирование
2	Тема 2. Итераторы и генераторы	Тестирование
3	Тема 3. Чтение больших файлов	Тестирование
4	Тема 4. Фильтры	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1. Каково основное назначение модуля в Python?

- А) Хранить только числовые данные
- Б) Объединять связанный программный код и обеспечивать его повторное использование
- В) Заменять операционную систему
- Г) Выполнять шифрование всех файлов автоматически

Вопрос 2. Какая инструкция используется для подключения модуля в Python?

- А) import
- Б) include
- В) connect
- Г) package

Вопрос 3. Какой специальный метод объекта возвращает итератор?

- А) __str__()
- Б) __iter__()
- В) __len__()
- Г) __main__()

Вопрос 4. Какое ключевое слово используется для выдачи очередного значения из генераторной функции?

- A) returnonly
- Б) yield
- В) break
- Г) pass

Вопрос 5. В чем преимущество генераторов при обработке больших последовательностей?

- A) Они обязательно сохраняют все элементы в памяти
- Б) Они формируют значения по мере необходимости и позволяют экономить память
- В) Они работают только со строками
- Г) Они автоматически шифруют данные

Вопрос 6. Какой подход наиболее рационален при чтении файла, размер которого существенно превышает доступную оперативную память?

- A) Считать весь файл одной операцией в строку
- Б) Читать файл построчно или блоками
- В) Скопировать файл несколько раз
- Г) Преобразовать весь файл в изображение

Вопрос 7. Для чего используется конструкция with open(...) при работе с файлами?

- A) Для автоматического закрытия файлового ресурса после завершения блока
- Б) Для обязательного запуска файла как программы
- В) Для удаления файла после чтения
- Г) Для сетевой передачи файла

Вопрос 8. Каково назначение функции filter() в Python?

- A) Сортировать элементы по возрастанию
- Б) Отбирать элементы последовательности, удовлетворяющие заданному условию
- В) Объединять несколько файлов
- Г) Создавать новый модуль

Вопрос 9. Что лучше использовать как предикат фильтрации, если условие сложное и должно повторно применяться в программе?

- A) Именованную функцию
- Б) Случайное число
- В) Только комментарий
- Г) Пустую строку

Вопрос 10. Какой вариант наиболее соответствует безопасной обработке журналов событий средствами Python?

- А) Обрабатывать входные данные без проверки ошибок
- Б) Использовать потоковое чтение, обработку исключений и фильтрацию записей по заданным критериям
- В) Загружать все журналы в память независимо от размера
- Г) Отключать проверку кодировки и структуры данных

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Компьютерные сети

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часа

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов построения и функционирования компьютерных сетей, моделей и протоколов сетевого взаимодействия, способов адресации и коммутации, а также практических умений выполнять базовую настройку сетевых устройств и применять информационно-коммуникационные технологии для организации надежной передачи данных и обеспечения защиты информации при ее передаче по компьютерным сетям.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-ИБ-2

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-ИБ-2

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост оятель ная работа	
1	Тема 1. Современные сетевые технологии	3	3	1	2	-
2	Тема 2. Базовая конфигурация коммутатора и конечного устройства	2	2	1	1	-
3	Тема 3. Протоколы и модели	2	2	1	1	-
4	Тема 4. Физический уровень	2	2	1	1	-
5	Тема 5. Системы счисления	2	2	0	2	-
6	Тема 6. Канальный уровень	2	2	1	1	-

7	Тема 7. Коммутация в сетях Ethernet	3	3	1	2	-
8	Тема 8. Сетевой уровень	2	2	1	1	-
9	Тема 9. Разрешение адресов	2	2	0	2	-
10	Тема 10. Базовая конфигурация маршрутизатора	3	3	1	2	-
11	Тема 11. IPv4-адресация	2	2	0	2	-
12	Тема 12. IPv6-адресация	2	2	0	2	-
13	Тема 13. ICMP: назначение и типы сообщений	2	2	0	2	-
14	Тема 14. ICMP: диагностика сетевого взаимодействия	2	2	0	2	-
15	Тема 15. Уровень приложений	3	3	0	3	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Современные сетевые технологии

- Понятие компьютерной сети и сетевой инфраструктуры
- Локальные и глобальные сети; проводные и беспроводные технологии
- Современные тенденции развития сетей и требования к защищенной передаче данных

Тема 2. Базовая конфигурация коммутатора и конечного устройства

- Назначение коммутатора и конечного устройства
- Доступ к CLI и основные режимы командной строки
- Настройка имени устройства, паролей, IP-параметров и проверка конфигурации

Тема 3. Протоколы и модели

- Модель OSI и стек TCP/IP
- Инкапсуляция и декапсуляция данных
- Назначение основных сетевых протоколов и взаимодействие уровней

Тема 4. Физический уровень

- Среды передачи данных и физические интерфейсы
- Характеристики медных, оптоволоконных и беспроводных каналов
- Кодирование, пропускная способность и факторы качества передачи

Тема 5. Системы счисления

- Двоичная, десятичная и шестнадцатеричная системы счисления
- Преобразование чисел между системами счисления
- Применение двоичного и шестнадцатеричного представления в сетевой адресации

Тема 6. Канальный уровень

- Функции канального уровня
- Структура Ethernet-кадра и MAC-адресация
- Контроль доступа к среде и обнаружение ошибок

Тема 7. Коммутация в сетях Ethernet

- Принципы работы Ethernet-коммутатора
- Таблица MAC-адресов: обучение, пересылка и фильтрация кадров
- Широковещательные домены и базовые особенности коммутации

Тема 8. Сетевой уровень

- Функции сетевого уровня
- IP-пакет и логическая адресация
- Маршрутизация и выбор пути доставки пакетов

Тема 9. Разрешение адресов

- Сопоставление сетевых и канальных адресов
- ARP в IPv4 и Neighbor Discovery в IPv6
- Анализ процесса разрешения адресов в локальной сети

Тема 10. Базовая конфигурация маршрутизатора

- Назначение и интерфейсы маршрутизатора
- Базовая настройка интерфейсов, шлюза и параметров доступа
- Проверка таблицы маршрутизации и сетевой связности

Тема 11. IPv4-адресация

- Структура IPv4-адреса и маски подсети
- Префикс сети, адрес сети, широковещательный адрес и диапазон узлов
- Основы подсетирования IPv4

Тема 12. IPv6-адресация

- Формат и запись IPv6-адресов
- Типы IPv6-адресов и правила сокращенной записи
- Базовая настройка и проверка IPv6-адресации

Тема 13. ICMP: назначение и типы сообщений

- Назначение протокола ICMP
- Основные типы и коды ICMP-сообщений
- Роль ICMP в сообщении об ошибках и контроле доступности

Тема 14. ICMP: диагностика сетевого взаимодействия

- Диагностические команды ping и traceroute/tracert
- Интерпретация ICMP-ответов и сообщений об ошибках
- Поиск типовых причин отсутствия сетевой связности

Тема 15. Уровень приложений

- Назначение прикладного уровня
- Протоколы DNS, DHCP, HTTP/HTTPS, электронной почты и передачи файлов
- Взаимодействие прикладных сервисов с транспортным и сетевым уровнями

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиокolonками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Современные сетевые технологии	Тестирование
2	Тема 2. Базовая конфигурация коммутатора и конечного устройства	Тестирование
3	Тема 3. Протоколы и модели	Тестирование
4	Тема 4. Физический уровень	Тестирование
5	Тема 5. Системы счисления	Тестирование
6	Тема 6. Канальный уровень	Тестирование
7	Тема 7. Коммутация в сетях Ethernet	Тестирование
8	Тема 8. Сетевой уровень	Тестирование
9	Тема 9. Разрешение адресов	Тестирование
10	Тема 10. Базовая конфигурация маршрутизатора	Тестирование
11	Тема 11. IPv4-адресация	Тестирование
12	Тема 12. IPv6-адресация	Тестирование
13	Тема 13. ICMP: назначение и типы сообщений	Тестирование
14	Тема 14. ICMP: диагностика сетевого взаимодействия	Тестирование
15	Тема 15. Уровень приложений	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какое устройство преимущественно используется для пересылки Ethernet-кадров внутри локальной сети?

- А) Маршрутизатор
- Б) Коммутатор
- В) DNS-сервер
- Г) Межсетевой экран

Вопрос 2 Какова основная функция модели OSI при изучении сетевого взаимодействия?

- А) Назначать IP-адреса автоматически
- Б) Определять физическую длину кабеля
- В) Разделять сетевое взаимодействие на функциональные уровни
- Г) Шифровать все передаваемые данные

Вопрос 3 Какой адрес используется коммутатором Ethernet для принятия решения о пересылке кадра?

- А) MAC-адрес
- Б) IPv4-адрес
- В) Номер TCP-порта
- Г) Имя DNS

Вопрос 4 Какой уровень модели OSI отвечает за логическую адресацию и маршрутизацию пакетов?

- А) Физический
- Б) Канальный
- В) Сетевой
- Г) Прикладной

Вопрос 5 Какой протокол используется в IPv4 для определения MAC-адреса узла по известному IPv4-адресу в локальной сети?

- А) DNS
- Б) ARP
- В) DHCP
- Г) HTTP

Вопрос 6 Какова длина IPv4-адреса?

- А) 16 бит
- Б) 32 бита
- В) 64 бита
- Г) 128 бит

Вопрос 7 Какова длина IPv6-адреса?

- А) 32 бита
- Б) 48 бит
- В) 64 бита
- Г) 128 бит

Вопрос 8 Для чего обычно применяется команда ping?

- А) Для проверки достижимости узла и времени отклика
- Б) Для изменения MAC-адреса коммутатора
- В) Для создания учетной записи пользователя
- Г) Для преобразования двоичного числа в десятичное

Вопрос 9 Какой протокол прикладного уровня преобразует доменные имена в IP-адреса?

- А) ICMP
- Б) Ethernet
- В) DNS
- Г) ARP

Вопрос 10 Какое действие наиболее непосредственно снижает риск несанкционированного доступа при базовой настройке сетевого устройства?

- А) Изменение имени файла конфигурации
- Б) Настройка аутентификации и защищенных паролей доступа
- В) Увеличение длины Ethernet-кадра
- Г) Отключение отображения IP-адресов

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Инструментальные средства разработки программного обеспечения

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 34 часа

Виды занятий	Объем часов
Лекции	8 часов
Самостоятельная работа	26 часов
Аттестация	Зачет
ВСЕГО:	34 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания современных инструментальных средств и технологий разработки программного обеспечения, а также практических умений применять языки программирования, интегрированные среды разработки, системы контроля версий, средства сборки, тестирования, отладки и анализа программ для решения задач профессиональной деятельности; формирование навыков проведения программных экспериментов по заданной методике, фиксации, обработки и интерпретации их результатов.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-ИБ-7
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-ИБ-7
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оятель- ная работа	
1	Тема 1. Интегрированные среды разработки и организация программного проекта	11	11	3	8	-
2	Тема 2. Системы контроля версий, сборки, тестирования и отладки программных средств	11	11	3	8	-
3	Тема 3. Программные эксперименты, профилирование и обработка результатов	12	12	2	10	-
	ВСЕГО	34	34	8	26	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Интегрированные среды разработки и организация программного проекта

- Назначение и классификация инструментальных средств разработки программного обеспечения.
- Интегрированные среды разработки (IDE): структура проекта, редактор кода, навигация, расширения и конфигурация среды.
- Языки программирования и средства автоматизации типовых операций разработки; организация зависимостей и конфигурационных файлов.
- Создание, запуск и сопровождение программного проекта с учетом требований к воспроизводимости среды разработки.

Тема 2. Системы контроля версий, сборки, тестирования и отладки программных средств

- Системы контроля версий: репозиторий, фиксация изменений, ветвление, слияние и разрешение конфликтов.
- Средства сборки и управления зависимостями; автоматизация компиляции, упаковки и запуска программных средств.
- Методы тестирования программного обеспечения и инструменты автоматизированного тестирования.
- Отладка программ: точки останова, пошаговое выполнение, анализ значений переменных, журналирование и диагностика ошибок.
- Основы совместной разработки и документирования изменений программного продукта.

Тема 3. Программные эксперименты, профилирование и обработка результатов

- Постановка программного эксперимента: цель, гипотеза, методика, входные данные, контролируемые параметры и критерии оценки.
- Инструменты профилирования и измерения характеристик программ: время выполнения, использование памяти и других ресурсов.
- Сбор, фиксация и подготовка экспериментальных данных к обработке.
- Обработка результатов: сравнение вариантов реализации, расчет показателей, представление результатов в таблицах и графиках.
- Интерпретация результатов эксперимента, выявление ограничений методики и формулирование обоснованных выводов.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Интегрированные среды разработки и организация программного проекта	Тестирование
2	Тема 2. Системы контроля версий, сборки, тестирования и отладки программных средств	Тестирование
3	Тема 3. Программные эксперименты, профилирование и обработка результатов	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Каково основное назначение интегрированной среды разработки (IDE)?

- А) Только хранение резервных копий файлов
- Б) Объединение средств редактирования, запуска, отладки и управления проектом
- В) Только публикация готовых программ в сети Интернет
- Г) Замена языка программирования операционной системой

Вопрос 2 Какое действие в системе контроля версий создает зафиксированное состояние набора изменений в репозитории?

- А) Commit
- Б) Debug
- В) Compile
- Г) Profile

Вопрос 3 Для чего применяется ветвление (branching) в системе контроля версий?

- А) Для удаления исходного кода после сборки
- Б) Для независимой разработки изменений без немедленного воздействия на основную линию проекта
- В) Для измерения скорости процессора
- Г) Для автоматического шифрования всех файлов проекта

Вопрос 4 Какова основная функция системы сборки программного обеспечения?

- А) Автоматизация преобразования исходного кода и зависимостей в готовый к запуску или распространению результат
- Б) Создание учетных записей пользователей
- В) Замена тестирования программного обеспечения
- Г) Назначение сетевых адресов

Вопрос 5 Какой инструментальный прием наиболее непосредственно помогает найти место возникновения ошибки во время выполнения программы?

- А) Пошаговая отладка с точками останова
- Б) Архивирование исходного кода
- В) Переименование каталога проекта
- Г) Удаление журнала событий

Вопрос 6 Что является основным назначением автоматизированного тестирования?

- А) Исключить необходимость формулировать ожидаемый результат
- Б) Повторяемо проверять соответствие поведения программы заданным условиям
- В) Заменить систему контроля версий
- Г) Увеличить объем исходного кода

Вопрос 7 Что необходимо определить до начала эксперимента с программным средством?

- А) Только название файла результата

- Б) Цель, методику, изменяемые параметры и критерии оценки
- В) Только используемый шрифт интерфейса
- Г) Только версию операционной системы пользователя

Вопрос 8 Для чего применяется профилировщик программного обеспечения?

- А) Для измерения характеристик выполнения программы и поиска ресурсоемких участков
- Б) Для создания новых языков программирования
- В) Для выдачи IP-адресов
- Г) Для шифрования документации

Вопрос 9 Какой подход повышает воспроизводимость программного эксперимента?

- А) Изменение нескольких параметров без фиксации их значений
- Б) Фиксация версии программы, входных данных, параметров среды и последовательности действий
- В) Удаление результатов предыдущих запусков без сохранения
- Г) Проведение каждого запуска по новой методике

Вопрос 10 Как следует обрабатывать результаты серии программных экспериментов?

- А) Выбирать только результат, подтверждающий исходную гипотезу
- Б) Сопоставлять результаты по единым критериям, выявлять различия и формулировать выводы с учетом условий эксперимента
- В) Игнорировать повторные измерения
- Г) Оценивать результат только по названию используемого инструмента

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Прикладная математика

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 144 часа

Виды занятий	Объем часов
Лекции	28 часов
Самостоятельная работа	116 часов
Аттестация	Зачет
ВСЕГО:	144 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания и практических навыков применения математических методов для решения задач профессиональной деятельности в области информационных технологий и информационной безопасности; освоение методов математического моделирования, анализа количественных зависимостей, вероятностно-статистической обработки данных, а также обработки и интерпретации результатов экспериментов, проводимых по заданной методике.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-ИБ-3
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-ИБ-3
2	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-ИБ-11

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оятель- ная работа	
1	Тема 1. Линейная алгебра, аналитическая геометрия и математические модели	48	48	9	39	-
2	Тема 2. Дифференциальное и интегральное исчисление. Методы оптимизации	48	48	9	39	-
3	Тема 3. Теория вероятностей, математическая статистика и обработка результатов эксперимента	48	48	10	38	-
	ВСЕГО	144	144	28	116	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Линейная алгебра, аналитическая геометрия и математические модели

- Матрицы, определители и системы линейных алгебраических уравнений; методы их решения.

- Векторы и операции над ними. Скалярное произведение, линейная зависимость и базис.
- Элементы аналитической геометрии: прямые, плоскости, расстояния и углы.
- Построение математических моделей профессиональных задач с использованием систем уравнений и матричного аппарата.
- Интерпретация результатов расчетов и оценка применимости выбранной математической модели.

Тема 2. Дифференциальное и интегральное исчисление. Методы оптимизации

- Функции одной и нескольких переменных, предел и непрерывность.
- Производная и дифференциал. Исследование функций и оценка скорости изменения параметров.
- Неопределенный и определенный интеграл, основные методы интегрирования.
- Частные производные и градиент. Задачи поиска экстремума функций нескольких переменных.
- Основы математической оптимизации и применение оптимизационных методов к прикладным задачам.

Тема 3. Теория вероятностей, математическая статистика и обработка результатов эксперимента

- Случайные события, вероятности и основные правила их вычисления.
- Случайные величины и числовые характеристики: математическое ожидание, дисперсия и среднее квадратическое отклонение.
- Выборочные данные и описательная статистика. Представление результатов наблюдений.
- Статистические оценки и проверка статистических гипотез по заданной методике.
- Обработка результатов эксперимента: группировка данных, расчет показателей, сравнение серий измерений и оценка разброса.
- Интерпретация экспериментальных результатов и формулирование выводов с учетом ограничений применяемых методов.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
--	-----------------------------------	----------

1	Тема 1. Линейная алгебра, аналитическая геометрия и математические модели	Тестирование
2	Тема 2. Дифференциальное и интегральное исчисление. Методы оптимизации	Тестирование
3	Тема 3. Теория вероятностей, математическая статистика и обработка результатов эксперимента	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какой математический объект используется для компактного представления системы линейных уравнений?

- А) Матрица
- Б) Логарифм
- В) Производная
- Г) Случайное событие

Вопрос 2 Какое условие гарантирует единственность решения квадратной системы линейных уравнений?

- А) Определитель матрицы коэффициентов не равен нулю
- Б) Все коэффициенты равны нулю
- В) Число уравнений всегда меньше числа неизвестных
- Г) В системе отсутствует свободный член

Вопрос 3 Что характеризует скалярное произведение двух векторов?

- А) Взаимосвязь длин векторов и угла между ними
- Б) Только количество координат
- В) Значение определенного интеграла
- Г) Вероятность случайного события

Вопрос 4 Каков геометрический смысл производной функции одной переменной в точке?

- А) Тангенс угла наклона касательной к графику функции
- Б) Площадь под графиком функции
- В) Среднее значение выборки
- Г) Определитель матрицы

Вопрос 5 Для чего в прикладных задачах используется градиент функции нескольких переменных?

- А) Для определения направления наиболее быстрого возрастания функции
- Б) Для вычисления количества строк матрицы
- В) Для определения вероятности невозможного события
- Г) Для преобразования случайной величины в константу

Вопрос 6 Что выражает определенный интеграл в типичной геометрической интерпретации?

- А) Ориентированную площадь между графиком функции и осью на заданном интервале
- Б) Угол между двумя векторами
- В) Число независимых испытаний
- Г) Ранг матрицы

Вопрос 7 Какое значение имеет вероятность достоверного события?

- А) 1
- Б) 0
- В) -1
- Г) 100 независимо от шкалы

Вопрос 8 Что показывает дисперсия случайной величины?

- А) Степень разброса значений относительно математического ожидания
- Б) Только максимальное наблюдаемое значение
- В) Количество переменных в модели
- Г) Направление градиента

Вопрос 9 Что необходимо сделать для корректной обработки результатов серии экспериментов по заданной методике?

- А) Использовать единые критерии обработки и фиксировать условия проведения измерений
- Б) Исключать все результаты, не подтверждающие ожидания
- В) Изменять методику после каждого измерения без фиксации изменений
- Г) Анализировать только один случайно выбранный результат

Вопрос 10 Какой показатель обычно используется для оценки среднего значения выборочных наблюдений?

- А) Выборочное среднее
- Б) Определитель
- В) Градиент
- Г) Матрица перехода

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Экономика и управление

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 72 часа

Виды занятий	Объем часов
Лекции	20 часов
Самостоятельная работа	52 часа
Аттестация	Зачет
ВСЕГО:	72 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания экономических и управленческих основ профессиональной деятельности, необходимых для участия в формировании и реализации политики информационной безопасности, планирования и организации комплекса мер по защите информации, оценки ресурсов и рисков, а также подготовки исходных данных и технико-экономического обоснования проектных решений по созданию и развитию подсистем и средств обеспечения информационной безопасности.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-ИБ-10
2	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-ИБ-12

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-ИБ-10
2	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-ИБ-12

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Экономические основы деятельности организации и управления ресурсами	24	24	7	17	-
2	Тема 2. Управление	24	24	7	17	-

	организацией, проектами и рисками в сфере информационной безопасности					
3	Тема 3. Техничко-экономическое обоснование решений по обеспечению информационной безопасности	24	24	6	18	-
	ВСЕГО	72	72	20	52	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Экономические основы деятельности организации и управления ресурсами

- Организация как экономическая система: цели, ресурсы, процессы и результаты деятельности.
- Основные экономические категории: затраты, себестоимость, цена, доход, прибыль и рентабельность.
- Ресурсное обеспечение деятельности организации: трудовые, материальные, финансовые и информационные ресурсы.
- Бюджетирование и планирование затрат. Формирование смет и контроль исполнения бюджета.
- Экономическая эффективность управленческих решений и основные показатели ее оценки.

Тема 2. Управление организацией, проектами и рисками в сфере информационной безопасности

- Функции и методы управления: планирование, организация, мотивация, контроль и координация.
- Организационные структуры и распределение ответственности при реализации мероприятий по информационной безопасности.
- Основы проектного управления: цели, сроки, ресурсы, участники, контроль выполнения и отчетность.
- Управление рисками: выявление, оценка, выбор мер реагирования и контроль остаточного риска.
- Организация и поддержание выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
- Участие технического специалиста в формировании и реализации политики информационной безопасности.

Тема 3. Техничко-экономическое обоснование решений по обеспечению информационной безопасности

- Исходные данные для проектирования подсистем и средств обеспечения защиты информации.
- Структура затрат на создание, внедрение, эксплуатацию и сопровождение средств защиты информации.
- Методы сравнения альтернативных проектных решений по экономическим и техническим критериям.
- Показатели технико-экономической эффективности: совокупная стоимость владения, срок окупаемости, эффект от снижения рисков и предотвращенных потерь.
- Подготовка технико-экономического обоснования проектного решения: состав, логика расчетов и представление результатов.
- Учет ограничений, допущений и неопределенности при обосновании решений в области информационной безопасности.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Экономические основы деятельности организации и управления ресурсами	Тестирование
2	Тема 2. Управление организацией, проектами и рисками в сфере информационной безопасности	Тестирование
3	Тема 3. Техничко-экономическое обоснование решений по обеспечению информационной безопасности	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какой показатель отражает разницу между доходами организации и ее расходами за определенный период?

- А) Прибыль
- Б) Себестоимость
- В) Амортизация
- Г) Ликвидность

Вопрос 2 Что относится к основным функциям управления?

- А) Планирование, организация, мотивация и контроль
- Б) Только закупка оборудования
- В) Только бухгалтерский учет
- Г) Только техническое обслуживание

Вопрос 3 Что понимается под бюджетом проекта?

- А) Планом доходов и расходов, связанных с реализацией проекта
- Б) Перечнем нормативных документов
- В) Списком сотрудников организации
- Г) Графиком отпусков участников проекта

Вопрос 4 Какова основная цель управления рисками?

- А) Выявить и оценить риски, выбрать меры реагирования и контролировать их реализацию
- Б) Полностью исключить любые изменения проекта
- В) Увеличить число отчетных документов
- Г) Заменить технические меры организационными во всех случаях

Вопрос 5 Что характеризует совокупная стоимость владения решением?

- А) Все затраты на приобретение, внедрение, эксплуатацию и сопровождение за период использования
- Б) Только цену приобретения оборудования
- В) Только стоимость лицензии за первый год
- Г) Только расходы на обучение персонала

Вопрос 6 Что является исходными данными для технико-экономического обоснования решения по защите информации?

- А) Требования к защите, характеристики объекта, варианты решений, затраты и ожидаемый эффект
- Б) Только название средства защиты
- В) Только штатное расписание организации
- Г) Только рекламные материалы поставщика

Вопрос 7 Какой показатель может использоваться для сравнения альтернативных проектных решений?

- А) Срок окупаемости
- Б) Номер версии документа
- В) Количество страниц инструкции
- Г) Название подразделения

Вопрос 8 В чем состоит роль технического специалиста при формировании политики информационной безопасности?

- А) Участвовать в подготовке технически обоснованных требований и мер, необходимых для реализации политики
- Б) Единолично утверждать финансовую отчетность организации
- В) Самостоятельно менять организационную структуру компании
- Г) Выполнять только закупку оборудования

Вопрос 9 Что следует учитывать при оценке экономической эффективности мер информационной безопасности?

- А) Затраты на меры и ожидаемое снижение возможного ущерба и рисков
- Б) Только стоимость оборудования
- В) Только число сотрудников службы безопасности
- Г) Только продолжительность проекта

Вопрос 10 Для чего в технико-экономическом обосновании фиксируют ограничения и допущения?

- А) Чтобы обеспечить прозрачность расчетов и корректно интерпретировать их результаты
- Б) Чтобы исключить необходимость исходных данных
- В) Чтобы отказаться от сравнения вариантов
- Г) Чтобы автоматически гарантировать окупаемость проекта

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы алгоритмизации и программирования

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ
ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 144 часа

Виды занятий	Объем часов
Лекции	28 часов
Самостоятельная работа	116 часов
Аттестация	Зачет
ВСЕГО:	144 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов алгоритмизации и практических навыков разработки программных решений для задач профессиональной деятельности; освоение базовых алгоритмических конструкций, способов представления и обработки данных, приемов декомпозиции задач, написания, тестирования и отладки программ, а также применения математических методов при проектировании и оценке алгоритмов.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-ИБ-3
2	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-ИБ-7

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-ИБ-3
2	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-ИБ-7

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Основы алгоритмизации и базовые управляющие конструкции	48	48	9	39	-
2	Тема 2. Структуры данных, функции и модульная организация программ	48	48	9	39	-
3	Тема 3. Разработка, тестирование и отладка программных решений	48	48	10	38	-
	ВСЕГО	144	144	28	116	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Основы алгоритмизации и базовые управляющие конструкции

- Понятие алгоритма, его свойства и способы представления: словесное описание, блок-схемы, псевдокод.
- Этапы решения задачи на компьютере: постановка задачи, формализация, выбор метода, разработка алгоритма и программная реализация.
- Переменные, типы данных, выражения и операции. Ввод и вывод данных.
- Линейные, разветвляющиеся и циклические алгоритмы.

- Применение математических методов при построении вычислительных алгоритмов и оценке корректности результатов.

Тема 2. Структуры данных, функции и модульная организация программ

- Массивы и последовательности данных. Основные операции поиска, отбора и преобразования элементов.
- Строки, коллекции и базовые структуры данных, используемые при разработке программ.
- Функции и процедуры: параметры, возвращаемые значения, область видимости и повторное использование кода.
- Декомпозиция задачи и модульная организация программного решения.
- Основы оценки сложности алгоритмов и выбора рационального способа обработки данных.

Тема 3. Разработка, тестирование и отладка программных решений

- Жизненный цикл разработки небольшой программы: постановка требований, проектирование, реализация и проверка результата.
- Синтаксические, логические и ошибки времени выполнения. Приемы поиска и локализации ошибок.
- Тестирование программ: тестовые данные, граничные случаи и проверка ожидаемого результата.
- Использование средств отладки и пошагового выполнения программы.
- Рефакторинг и повышение читаемости программного кода.
- Разработка программных решений для типовых задач профессиональной деятельности с использованием изученных алгоритмических конструкций.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Основы алгоритмизации и базовые управляющие конструкции	Тестирование
2	Тема 2. Структуры данных, функции и модульная организация программ	Тестирование
3	Тема 3. Разработка, тестирование и отладка программных решений	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какое свойство алгоритма означает возможность разделить процесс решения задачи на отдельные шаги?

- А) Дискретность
- Б) Случайность
- В) Непрерывность
- Г) Избыточность

Вопрос 2 Какая алгоритмическая конструкция используется для выбора одного из вариантов действий в зависимости от условия?

- А) Ветвление
- Б) Последовательность
- В) Комментарий
- Г) Объявление типа

Вопрос 3 Какой цикл целесообразно использовать, когда число повторений заранее известно?

- А) Цикл со счетчиком
- Б) Только бесконечный цикл
- В) Ветвление
- Г) Рекурсивный вызов без условия завершения

Вопрос 4 Для чего в программе используются функции и процедуры?

- А) Для декомпозиции задачи и повторного использования кода
- Б) Только для хранения комментариев
- В) Только для изменения имени файла
- Г) Для запрета передачи параметров

Вопрос 5 Что называется массивом?

- А) Структура данных для хранения набора однотипных элементов
- Б) Единственная логическая переменная
- В) Оператор условного перехода
- Г) Ошибка времени выполнения

Вопрос 6 Что означает декомпозиция программной задачи?

- А) Разбиение сложной задачи на более простые подзадачи
- Б) Удаление всех функций из программы
- В) Замена алгоритма набором случайных действий
- Г) Исключение этапа тестирования

Вопрос 7 Какой тип ошибки возникает, если программа запускается, но выдает неверный результат?

- А) Логическая ошибка
- Б) Только синтаксическая ошибка
- В) Ошибка форматирования документа
- Г) Ошибка имени файла

Вопрос 8 Для чего используются граничные тестовые значения?

- А) Для проверки поведения программы на краях допустимого диапазона данных
- Б) Для увеличения размера исходного кода
- В) Для удаления всех проверок условий
- Г) Для замены алгоритма документацией

Вопрос 9 Что позволяет сделать пошаговая отладка программы?

- А) Последовательно выполнять инструкции и наблюдать изменение значений переменных
- Б) Автоматически доказать оптимальность любого алгоритма
- В) Исключить необходимость тестовых данных
- Г) Преобразовать исходный код в текстовый документ

Вопрос 10 Что характеризует временная сложность алгоритма?

- А) Зависимость количества выполняемых операций от размера входных данных
- Б) Цвет интерфейса среды разработки
- В) Количество комментариев в программе
- Г) Длину имени переменной

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 72 часа

Виды занятий	Объем часов
Лекции	20 часов
Самостоятельная работа	52 часа
Аттестация	Зачет
ВСЕГО:	72 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов эксплуатации автоматизированных (информационных) систем в защищенном исполнении, а также практических умений по администрированию средств защиты информации, поддержанию установленного уровня защищенности, контролю функционирования механизмов защиты и организации защиты информации ограниченного доступа в соответствии с требованиями нормативных правовых актов, нормативных и методических документов ФСБ России и ФСТЭК России.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России и ФСТЭК России	ОПК-ИБ-6

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-ИБ-1.2
2	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России и ФСТЭК России	ОПК-ИБ-6

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оятель- ная работа	
1	Тема 1. Организация эксплуатации автоматизированных систем в защищенном исполнении	24	24	7	17	-
2	Тема 2. Администрирование и контроль функционирования средств защиты информации	24	24	7	17	-
3	Тема 3. Обеспечение защиты информации ограниченного доступа при эксплуатации защищенных систем	24	24	6	18	-
	ВСЕГО	72	72	20	52	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Организация эксплуатации автоматизированных систем в защищенном исполнении

- Назначение и особенности автоматизированных (информационных) систем в защищенном исполнении.
- Эксплуатационная документация, состав и назначение организационно-распорядительных и технических документов.
- Режимы эксплуатации защищенной системы и требования к поддержанию установленного уровня защищенности.
- Порядок ввода в эксплуатацию, сопровождения, изменения конфигурации и вывода из эксплуатации компонентов системы.
- Распределение ролей и ответственности персонала при эксплуатации защищенной автоматизированной системы.
- Контроль соблюдения установленных требований безопасности в процессе эксплуатации.

Тема 2. Администрирование и контроль функционирования средств защиты информации

- Состав и назначение средств защиты информации в компьютерных системах и сетях.
- Администрирование механизмов идентификации, аутентификации, разграничения доступа и регистрации событий безопасности.
- Настройка и сопровождение средств антивирусной защиты, межсетевого экранирования и контроля сетевого взаимодействия.
- Управление учетными записями, правами доступа и параметрами безопасности в защищенной системе.
- Мониторинг состояния средств защиты информации, анализ журналов событий и выявление отклонений в работе механизмов защиты.
- Резервное копирование конфигураций, восстановление работоспособности и документирование изменений в настройках средств защиты.

Тема 3. Обеспечение защиты информации ограниченного доступа при эксплуатации защищенных систем

- Основные требования законодательства Российской Федерации к защите информации ограниченного доступа.
- Нормативные и методические документы ФСБ России и ФСТЭК России, применяемые при организации защиты информации.
- Организационные и технические меры защиты информации при эксплуатации автоматизированных систем.
- Контроль доступа к защищаемой информации, учет носителей и соблюдение установленных режимов обработки данных.
- Порядок реагирования на инциденты информационной безопасности, нарушения установленных правил и нештатные ситуации.
- Контроль эффективности принятых мер защиты, оформление результатов проверок и корректирующих мероприятий.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Организация эксплуатации автоматизированных систем в защищенном исполнении	Тестирование
2	Тема 2. Администрирование и контроль функционирования средств защиты информации	Тестирование
3	Тема 3. Обеспечение защиты информации ограниченного доступа при эксплуатации защищенных систем	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какова основная задача эксплуатации автоматизированной системы в защищенном исполнении?

- А) Поддержание работоспособности системы и установленного уровня ее защищенности
- Б) Только увеличение производительности серверов
- В) Только обновление пользовательского интерфейса
- Г) Исключительно закупка нового оборудования

Вопрос 2 Какой документ определяет порядок действий персонала при эксплуатации защищенной системы?

- А) Эксплуатационная и организационно-распорядительная документация
- Б) Рекламный буклет производителя
- В) Прайс-лист поставщика
- Г) Личный календарь администратора

Вопрос 3 Что относится к функциям администрирования средств защиты информации?

- А) Настройка параметров защиты, учетных записей, прав доступа и контроль состояния средств защиты
- Б) Только разработка дизайна интерфейса
- В) Только подготовка презентаций
- Г) Только замена офисной мебели

Вопрос 4 Для чего используются журналы регистрации событий безопасности?

- А) Для контроля действий и выявления событий, имеющих значение для безопасности
- Б) Для хранения графических файлов пользователей
- В) Для учета рабочего времени бухгалтерии
- Г) Для настройки яркости мониторов

Вопрос 5 Какой принцип должен соблюдаться при предоставлении пользователю прав доступа?

- А) Предоставление только тех прав, которые необходимы для выполнения служебных обязанностей
- Б) Предоставление максимальных прав всем пользователям
- В) Полный отказ от разграничения доступа

Г) Использование одной учетной записи всеми сотрудниками

Вопрос 6 Что необходимо сделать перед внесением существенных изменений в конфигурацию средств защиты?

- А) Оценить влияние изменений, зафиксировать их и обеспечить возможность восстановления конфигурации
- Б) Удалить все журналы событий
- В) Отключить все защитные механизмы без документирования
- Г) Передать права администратора всем пользователям

Вопрос 7 Какие документы должны учитываться при организации защиты информации ограниченного доступа?

- А) Нормативные правовые акты, а также применимые нормативные и методические документы ФСБ России и ФСТЭК России
- Б) Только внутренние рекламные материалы
- В) Только инструкции производителя офисной техники
- Г) Любые публикации из социальных сетей

Вопрос 8 Что является одной из организационных мер защиты информации?

- А) Разграничение полномочий и установление порядка доступа к защищаемой информации
- Б) Увеличение разрешения экрана
- В) Замена клавиатур
- Г) Использование одинаковых паролей всеми сотрудниками

Вопрос 9 Что следует сделать при выявлении инцидента информационной безопасности?

- А) Зафиксировать событие и действовать в соответствии с установленным порядком реагирования
- Б) Игнорировать событие, если система продолжает работать
- В) Удалить все журналы регистрации
- Г) Немедленно предоставить пользователям дополнительные права

Вопрос 10 Для чего проводится контроль эффективности мер защиты информации?

- А) Для подтверждения работоспособности и достаточности принятых мер и выявления необходимости корректирующих действий
- Б) Только для увеличения объема отчетности
- В) Только для проверки скорости интернет-соединения
- Г) Для отказа от дальнейшего администрирования системы

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Сети и системы передачи информации

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость:

72 часа

Виды занятий

Объем часов

Лекции	20 часов
Самостоятельная работа	52 часа
Аттестация	Зачет
ВСЕГО:	72 часа

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов построения, функционирования и передачи информации в компьютерных сетях и системах связи, а также практических умений применять физические законы и модели для анализа процессов передачи сигналов, выбирать и использовать сетевые технологии и протоколы, обеспечивать защиту информации при ее передаче по компьютерным сетям и оценивать параметры надежности и безопасности сетевого взаимодействия.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-ИБ-4

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-ИБ-1.3
2	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-ИБ-4

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Основы построения компьютерных сетей и физические основы передачи данных	24	24	7	17	-
2	Тема 2. Сетевые протоколы, адресация и организация передачи информации	24	24	7	17	-
3	Тема 3. Надежность и защита информации в сетях и системах передачи данных	24	24	6	18	-
	ВСЕГО	72	72	20	52	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Основы построения компьютерных сетей и физические основы передачи данных

- Назначение и классификация компьютерных сетей и систем передачи информации.
- Основные элементы сетевой инфраструктуры: узлы, каналы связи, активное и пассивное сетевое оборудование.

- Физические основы передачи сигналов: аналоговые и цифровые сигналы, полоса пропускания, затухание, помехи и отношение сигнал/шум.
- Среды передачи данных: медные кабели, волоконно-оптические линии и беспроводные каналы.
- Пропускная способность канала и факторы, влияющие на скорость и качество передачи данных.
- Базовые топологии сетей и принципы выбора структуры сети для решения профессиональных задач.

Тема 2. Сетевые протоколы, адресация и организация передачи информации

- Многоуровневые модели сетевого взаимодействия OSI и TCP/IP.
- Назначение и взаимодействие протоколов канального, сетевого, транспортного и прикладного уровней.
- Принципы адресации в сетях: MAC-адреса, IPv4 и IPv6, подсети и маршрутизация.
- Коммутация и маршрутизация пакетов, основные алгоритмы продвижения данных.
- Транспортные протоколы TCP и UDP, управление соединением и контроль доставки.
- Диагностика сетевого взаимодействия с использованием служебных протоколов и инструментов анализа трафика.

Тема 3. Надежность и защита информации в сетях и системах передачи данных

- Угрозы безопасности информации при передаче по компьютерным сетям.
- Принципы обеспечения конфиденциальности, целостности и доступности данных в сетевом взаимодействии.
- Механизмы аутентификации, управления доступом и защиты сетевых соединений.
- Использование криптографических протоколов и защищенных каналов передачи данных.
- Методы повышения надежности сетей: резервирование каналов, отказоустойчивость и контроль доступности сервисов.
- Анализ сетевых событий и трафика, выявление отклонений и оценка эффективности мер защиты информации.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
--	-----------------------------------	----------

1	Тема 1. Основы построения компьютерных сетей и физические основы передачи данных	Тестирование
2	Тема 2. Сетевые протоколы, адресация и организация передачи информации	Тестирование
3	Тема 3. Надежность и защита информации в сетях и системах передачи данных	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что в компьютерной сети называется пропускной способностью канала связи?

- А) Максимальный объем данных, который может быть передан по каналу за единицу времени
- Б) Количество сетевых устройств в помещении
- В) Длина сетевого имени компьютера
- Г) Число пользователей операционной системы

Вопрос 2 Какой фактор непосредственно приводит к ослаблению сигнала при его распространении по линии связи?

- А) Затухание
- Б) Адресация
- В) Маршрутизация
- Г) Инкапсуляция

Вопрос 3 На каком уровне модели OSI выполняется логическая адресация и маршрутизация пакетов?

- А) Сетевом
- Б) Физическом
- В) Представления
- Г) Сеансовом

Вопрос 4 Какова основная функция IP-адреса?

- А) Логическая идентификация узла и его местоположения в IP-сети
- Б) Шифрование содержимого пакета
- В) Определение производителя сетевой карты
- Г) Контроль температуры сетевого оборудования

Вопрос 5 Какое основное отличие TCP от UDP?

- А) TCP обеспечивает установление соединения и контроль доставки данных
- Б) UDP всегда шифрует данные, а TCP нет
- В) TCP работает только в локальных сетях
- Г) UDP использует только IPv6

Вопрос 6 Какой механизм помогает обеспечить конфиденциальность данных при передаче по недоверенной сети?

- А) Шифрование сетевого соединения
- Б) Увеличение длины кабеля
- В) Изменение имени рабочей станции
- Г) Повышение яркости монитора

Вопрос 7 Что означает принцип целостности информации в сетевом взаимодействии?

- А) Защиту данных от несанкционированного изменения
- Б) Гарантию неограниченного доступа всех пользователей
- В) Увеличение скорости передачи до максимума
- Г) Хранение данных только в одном экземпляре

Вопрос 8 Для чего применяется резервирование каналов связи?

- А) Для повышения доступности и отказоустойчивости сети
- Б) Для уменьшения количества IP-адресов
- В) Для замены аутентификации пользователей
- Г) Для отключения журналирования событий

Вопрос 9 Какой инструментальный подход используется для анализа сетевого трафика и выявления аномалий?

- А) Перехват и исследование пакетов с помощью анализатора сетевого трафика
- Б) Изменение разрешения экрана
- В) Архивация текстовых документов
- Г) Форматирование локального диска

Вопрос 10 Что необходимо учитывать при выборе мер защиты информации в сети?

- А) Характер угроз, свойства обрабатываемой информации, архитектуру сети и требования к защите
- Б) Только цвет сетевого оборудования
- В) Только количество мониторов
- Г) Только версию офисного пакета

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Электроника и схемотехника

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 108 часов

Виды занятий	Объем часов
Лекции	22 часа
Самостоятельная работа	86 часов
Аттестация	Зачет
ВСЕГО:	108 часов

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания физических принципов работы электронных компонентов и схем, методов анализа и расчета электрических и электронных цепей, а также практических умений применять законы и модели электротехники и электроники при решении профессиональных задач, оценивать параметры электронных устройств и использовать средства технической и криптографической защиты информации с учетом аппаратной реализации и условий эксплуатации.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-ИБ-4
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-ИБ-4
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Основы электрических цепей и полупроводниковой электроники	36	36	7	29	-
2	Тема 2. Аналоговые и цифровые электронные устройства и схемы	36	36	7	29	-
3	Тема 3. Аппаратные средства технической и криптографической защиты информации	36	36	8	28	-
	ВСЕГО	108	108	22	86	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Основы электрических цепей и полупроводниковой электроники

- Основные электрические величины и параметры: ток, напряжение, сопротивление, мощность и энергия.
- Законы Ома и Кирхгофа, методы расчета линейных электрических цепей постоянного и переменного тока.
- Пассивные элементы электронных схем: резисторы, конденсаторы, индуктивности; их характеристики и применение.
- Полупроводниковые материалы и p-n-переход. Диоды, стабилитроны и выпрямительные схемы.
- Биполярные и полевые транзисторы: принципы действия, режимы работы и базовые схемы включения.
- Измерение и оценка параметров электрических и электронных цепей.

Тема 2. Аналоговые и цифровые электронные устройства и схемы

- Аналоговые усилительные каскады и основные параметры усилителей.

- Операционные усилители и типовые схемы их применения: усиление, суммирование, фильтрация и сравнение сигналов.
- Генераторы, стабилизаторы и источники питания электронных устройств.
- Основы цифровой схемотехники: логические уровни, базовые логические элементы и булевы функции.
- Комбинационные и последовательностные цифровые устройства: дешифраторы, мультиплексоры, триггеры, регистры и счетчики.
- Основы аналого-цифрового и цифро-аналогового преобразования, интерфейсы сопряжения электронных устройств.

Тема 3. Аппаратные средства технической и криптографической защиты информации

- Аппаратные компоненты средств технической защиты информации и требования к их надежности.
- Технические каналы утечки информации и физические основы возникновения побочных электромагнитных излучений и наводок.
- Принципы экранирования, фильтрации, заземления и гальванической развязки в защищаемых электронных системах.
- Аппаратные средства криптографической защиты: назначение, типовые архитектуры и особенности применения.
- Контроль целостности, доверенная загрузка и аппаратные модули безопасности как элементы защищенных вычислительных систем.
- Диагностика, эксплуатационный контроль и оценка корректности функционирования электронных средств защиты информации.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Основы электрических цепей и полупроводниковой электроники	Тестирование
2	Тема 2. Аналоговые и цифровые электронные устройства и схемы	Тестирование
3	Тема 3. Аппаратные средства технической и криптографической защиты информации	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какой закон связывает ток, напряжение и сопротивление на участке электрической цепи?

- А) Закон Ома
- Б) Закон Фарадея
- В) Закон Архимеда
- Г) Закон Бойля-Мариотта

Вопрос 2 Какой элемент способен накапливать энергию электрического поля?

- А) Конденсатор
- Б) Резистор
- В) Диод
- Г) Предохранитель

Вопрос 3 Каково основное назначение полупроводникового диода в электрической цепи?

- А) Преимущественно проводить ток в одном направлении
- Б) Усиливать любой сигнал без питания
- В) Хранить цифровые данные
- Г) Измерять сопротивление

Вопрос 4 Для чего в электронных схемах часто применяется операционный усилитель?

- А) Для усиления и аналоговой обработки сигналов
- Б) Только для механического переключения контактов
- В) Для хранения электрической энергии
- Г) Для преобразования оптического сигнала в механический

Вопрос 5 Какой логический элемент выдает единицу только тогда, когда оба его входа равны единице?

- А) И (AND)
- Б) ИЛИ (OR)
- В) НЕ (NOT)
- Г) Исключающее ИЛИ (XOR)

Вопрос 6 Каково назначение аналого-цифрового преобразователя?

- А) Преобразование аналогового сигнала в цифровой код
- Б) Усиление сетевого напряжения
- В) Шифрование файлов без вычислений
- Г) Формирование механического движения

Вопрос 7 Какое средство уменьшает влияние электромагнитных помех и побочных излучений на защищаемую аппаратуру?

- А) Экранирование и фильтрация
- Б) Увеличение яркости дисплея
- В) Изменение имени пользователя
- Г) Архивирование файлов

Вопрос 8 Какова одна из функций аппаратного модуля безопасности в защищенной системе?

- А) Защищенное хранение и выполнение операций с криптографическими ключами
- Б) Увеличение тактовой частоты монитора
- В) Замена всех сетевых протоколов
- Г) Автоматическое редактирование документов

Вопрос 9 Для чего применяется гальваническая развязка в электронных системах?

- А) Для электрического разделения цепей и снижения передачи помех и опасных потенциалов
- Б) Для повышения разрешения экрана
- В) Для изменения IP-адреса
- Г) Для сжатия исполняемых файлов

Вопрос 10 Что следует контролировать при эксплуатации электронных средств защиты информации?

- А) Соответствие параметров установленным требованиям и корректность функционирования
- Б) Только внешний цвет корпуса
- В) Только количество подключенных клавиатур
- Г) Только размер рабочего стола операционной системы

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационно-правовое обеспечение информационной безопасности

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 108 часов

Виды занятий	Объем часов
Лекции	22 часа
Самостоятельная работа	86 часов
Аттестация	Зачет
ВСЕГО:	108 часов

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания правовых и организационных основ обеспечения информационной безопасности, умений применять нормативные правовые акты, нормативные и методические документы в профессиональной деятельности, организовывать защиту информации ограниченного доступа, разрабатывать и поддерживать организационно-распорядительную документацию, распределять ответственность и контролировать выполнение установленных требований по защите информации.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-ИБ-5
2	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России и ФСТЭК России	ОПК-ИБ-6

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-ИБ-5
2	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России и ФСТЭК России	ОПК-ИБ-6

1. Учебный план:

	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самостоятельная работа	
1	Тема 1. Нормативно-правовые основы обеспечения информационной безопасности	36	36	7	29	-
2	Тема 2. Организация защиты информации ограниченного доступа	36	36	7	29	-
3	Тема 3. Организационно-	36	36	8	28	-

	распорядительная документация и контроль выполнения требований информационной безопасности					
	ВСЕГО	108	108	22	86	
	Промежуточная аттестация	Тестирование				

2. Рабочие программы учебных предметов

Тема 1. Нормативно-правовые основы обеспечения информационной безопасности

- Система правового регулирования отношений в области информации, информационных технологий и защиты информации.
- Виды нормативных правовых актов, нормативных и методических документов в области информационной безопасности и их место в системе регулирования.
- Полномочия государственных органов и регуляторов в сфере защиты информации.
- Правовые режимы информации ограниченного доступа и общие требования к обеспечению ее конфиденциальности, целостности и доступности.
- Ответственность организаций и должностных лиц за нарушение установленных требований в области защиты информации.
- Применение требований нормативных документов при решении профессиональных задач по обеспечению информационной безопасности.

Тема 2. Организация защиты информации ограниченного доступа

- Организационные основы построения системы защиты информации на объекте защиты.
- Определение состава защищаемой информации, объектов информатизации, участников процессов и зон ответственности.
- Организация допуска и разграничения доступа к информации ограниченного доступа.
- Требования к защите информации в соответствии с нормативными и методическими документами ФСБ России и ФСТЭК России.
- Организация учета, хранения, передачи и уничтожения носителей информации ограниченного доступа.
- Порядок реагирования на нарушения режима защиты информации и взаимодействия ответственных подразделений.

Тема 3. Организационно-распорядительная документация и контроль выполнения требований информационной безопасности

- Назначение и состав организационно-распорядительной документации по информационной безопасности.
- Политики, положения, регламенты, инструкции, перечни и журналы как элементы документированного управления защитой информации.
- Распределение полномочий и ответственности между владельцами информационных ресурсов, администраторами и пользователями.
- Организация внутреннего контроля выполнения требований информационной безопасности и документирование результатов проверок.
- Актуализация локальных нормативных документов при изменении информационных систем, процессов и требований регуляторов.
- Подготовка мероприятий по устранению выявленных несоответствий и контроль их исполнения.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения. Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Нормативно-правовые основы обеспечения информационной безопасности	Тестирование
2	Тема 2. Организация защиты информации ограниченного доступа	Тестирование
3	Тема 3. Организационно-распорядительная документация и контроль выполнения требований информационной безопасности	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Что относится к нормативному правовому обеспечению информационной безопасности?

- А) Нормативные правовые акты, устанавливающие обязательные требования в области защиты информации
- Б) Только инструкции производителя оборудования
- В) Только пользовательские заметки
- Г) Только рекламные материалы

Вопрос 2 Какова основная цель организационных мер по защите информации?

- А) Установить порядок действий, полномочия и ответственность участников процессов защиты информации
- Б) Полностью заменить технические средства защиты
- В) Исключить необходимость контроля доступа
- Г) Отменить документирование процессов

Вопрос 3 Что необходимо определить до организации защиты информации ограниченного доступа?

- А) Состав защищаемой информации, объекты защиты и круг лиц, которым необходим доступ
- Б) Только модель монитора пользователя
- В) Только график отпусков сотрудников
- Г) Только способ архивирования открытых данных

Вопрос 4 Какой принцип должен применяться при предоставлении доступа к информации ограниченного доступа?

- А) Доступ предоставляется в объеме, необходимом для выполнения должностных обязанностей
- Б) Доступ предоставляется всем сотрудникам без ограничений
- В) Доступ определяется только стажем работы
- Г) Доступ не требует документального оформления

Вопрос 5 Для чего организации разрабатывают локальные документы по информационной безопасности?

- А) Для закрепления требований, процедур, ролей и ответственности внутри организации
- Б) Только для увеличения объема документооборота
- В) Для отмены требований законодательства
- Г) Для замены программного обеспечения

Вопрос 6 Что является примером организационно-распорядительного документа по информационной безопасности?

- А) Политика информационной безопасности
- Б) Рекламный буклет
- В) Каталог оборудования поставщика
- Г) Графический файл без утверждения

Вопрос 7 Что должно происходить при изменении нормативных требований или состава информационной системы?

- А) Должна проводиться оценка необходимости актуализации локальных документов и мер защиты
- Б) Все действующие документы автоматически утрачивают силу
- В) Изменения можно не учитывать до следующего десятилетия
- Г) Следует отменить контроль выполнения требований

Вопрос 8 Какова задача внутреннего контроля информационной безопасности?

- А) Проверять соблюдение установленных требований и фиксировать выявленные несоответствия
- Б) Только измерять производительность компьютеров
- В) Исключительно обучать новых сотрудников
- Г) Заменять все технические средства защиты

Вопрос 9 Кто должен быть определен в системе организационного обеспечения информационной безопасности?

- А) Ответственные лица, их полномочия и зоны ответственности
- Б) Только сотрудники бухгалтерии
- В) Только внешние поставщики
- Г) Только пользователи без административных полномочий

Вопрос 10 Что следует делать по результатам выявленного нарушения требований информационной безопасности?

- А) Зарегистрировать нарушение, определить корректирующие меры и проконтролировать их выполнение
- Б) Не документировать событие
- В) Удалить все локальные документы
- Г) Предоставить нарушителю дополнительные права доступа

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационно-правовое обеспечение информационной безопасности

ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Сетевые системы и защита данных

Вид профессиональной деятельности:

Защита информации в компьютерных системах и сетях

Трудоемкость: 180 часов

Виды занятий	Объем часов
Лекции	36 часов
Самостоятельная работа	144 часа
Аттестация	Зачет
ВСЕГО:	180 часов

Москва, 2026

Цель программы: Формирование у обучающихся системного понимания принципов и методов защиты информации в автоматизированных системах программными и программно-аппаратными средствами, практических умений разрабатывать и реализовывать политики управления доступом, применять средства криптографической и технической защиты информации, настраивать механизмы идентификации, аутентификации, разграничения доступа, регистрации и контроля событий безопасности при решении профессиональных задач.

Место дисциплины в структуре ДПП:

Дисциплина относится к числу профессиональных дисциплин и является частью дополнительной профессиональной программы – программы профессиональной переподготовки.

Совершенствуемые компетенции

№	Компетенция	ФГОС 10.03.01 Информационная безопасность
1	Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-ИБ-1.1
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

Планируемый результат обучения:

№ п/п	В результате освоения программы обучающийся должен	Код компетенций в соответствии с ФГОС 10.03.01 Информационная безопасность
1	2	3
1	Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-ИБ-1.1
2	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-ИБ-9

1. Учебный план:

	Наименование модулей по программе	Общая трудо- емкость (акад. часов)	Всего ауд.ч	В том числе		Форма ТА
				Лекции	Самост- оятель- ная работа	
1	Тема 1. Архитектура защищенных автоматизированных систем и модели угроз	36	36	7	29	-
2	Тема 2. Управление доступом, идентификация и аутентификация в автоматизированных системах	36	36	7	29	-
3	Тема 3. Программные средства защиты информации и контроль событий безопасности	36	36	7	29	-
4	Тема 4. Криптографические средства защиты информации в автоматизированных	36	36	7	29	-

	системах					
5	Тема 5. Программно-аппаратные средства технической защиты и комплексная эксплуатация системы защиты	36	36	7	29	
	ВСЕГО	180	180	36	144	

2. Рабочие программы учебных предметов

Тема 1. Архитектура защищенных автоматизированных систем и модели угроз

- Назначение и структура системы защиты информации автоматизированной системы.
- Основные компоненты автоматизированной системы и точки возникновения угроз безопасности информации.
- Модели угроз и нарушителя как основа выбора мер защиты.
- Принципы эшелонированной защиты и минимизации доверенной вычислительной базы.
- Взаимосвязь программных, программно-аппаратных и организационных мер защиты.

Тема 2. Управление доступом, идентификация и аутентификация в автоматизированных системах

- Идентификация и аутентификация субъектов доступа.
- Дискреционное, мандатное и ролевое управление доступом.
- Разработка политик управления доступом с учетом принципов минимальных привилегий и разделения обязанностей.
- Управление учетными записями, полномочиями и жизненным циклом прав доступа.
- Контроль корректности применения политик доступа в компьютерных системах.

Тема 3. Программные средства защиты информации и контроль событий безопасности

- Назначение и классы программных средств защиты информации.
- Средства антивирусной защиты, контроля целостности и предотвращения несанкционированного доступа.
- Регистрация и аудит событий безопасности, журналы и централизованный сбор событий.
- Настройка правил контроля, оповещения и реагирования на события безопасности.
- Оценка совместимости и эффективности программных средств защиты в составе автоматизированной системы.

Тема 4. Криптографические средства защиты информации в автоматизированных системах

- Назначение криптографической защиты информации и области ее применения.
- Шифрование данных при хранении и передаче, электронная подпись и контроль целостности.
- Основы управления криптографическими ключами и требования к их жизненному циклу.
- Применение криптографических средств в защищенных каналах связи и сервисах автоматизированных систем.
- Организационные и технические аспекты безопасной эксплуатации средств криптографической защиты.

Тема 5. Программно-аппаратные средства технической защиты и комплексная эксплуатация системы защиты

- Аппаратные и программно-аппаратные средства доверенной загрузки, аутентификации и контроля доступа.
- Средства межсетевое экранирования, обнаружения и предотвращения вторжений.
- Развертывание, настройка и сопровождение комплекса средств защиты информации.

- Контроль конфигураций, обновление программного обеспечения и резервирование критичных компонентов.
- Оценка состояния защищенности автоматизированной системы и корректировка применяемых мер защиты.

3. Условия реализации программы

3.1. Материально-технические условия реализации программы

Технические средства обучения

Компьютерное оборудование; видео- и аудиовизуальные средства обучения.

Наличие доступа слушателей к информационно-телекоммуникационной сети Интернет, оснащение компьютерным оборудованием: веб-камерой, микрофоном, аудиоколонками и (или) наушниками.

Консультационная и информационная поддержка обучающихся (слушателей) осуществляется с помощью электронной почты, современных сервисов Интернет взаимодействия.

Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

3.2. Требованиям к информационным и учебно-методическим условиям

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

- Электронная образовательная платформа ЮРАЙТ (ЭБС) <https://urait.ru/>;

Текущая аттестация:

Тестирование (выполнение заданий)

	Наименование модулей по программе	Форма ТА
1	Тема 1. Архитектура защищенных автоматизированных систем и модели угроз	Тестирование
2	Тема 2. Управление доступом, идентификация и аутентификация в автоматизированных системах	Тестирование
3	Тема 3. Программные средства защиты информации и контроль событий безопасности	Тестирование
4	Тема 4. Криптографические средства защиты информации в автоматизированных системах	Тестирование
5	Тема 5. Программно-аппаратные средства технической защиты и комплексная эксплуатация системы защиты	Тестирование

Промежуточная аттестация по курсу (Тестирование):

Вопрос 1 Какой принцип управления доступом предполагает предоставление пользователю только тех прав, которые необходимы для выполнения его задач?

- А) Принцип минимальных привилегий
- Б) Принцип открытого доступа
- В) Принцип неограниченного доверия
- Г) Принцип полного дублирования

Вопрос 2 Что определяет политика управления доступом?

- А) Правила предоставления, изменения и отзыва прав доступа к ресурсам
- Б) Только порядок резервного копирования

- В) Только правила размещения оборудования
- Г) Только требования к электропитанию

Вопрос 3 Какова основная функция средства контроля целостности?

- А) Выявление несанкционированных изменений контролируемых объектов
- Б) Увеличение пропускной способности сети
- В) Создание новых учетных записей
- Г) Замена криптографических ключей

Вопрос 4 Для чего применяется журналирование событий безопасности?

- А) Для регистрации действий и событий с целью последующего контроля и анализа
- Б) Для ускорения выполнения приложений
- В) Для автоматической замены аппаратных компонентов
- Г) Для отключения механизмов аутентификации

Вопрос 5 Какое средство относится к криптографической защите информации?

- А) Средство шифрования данных
- Б) Источник бесперебойного питания
- В) Система охлаждения
- Г) Кабельный тестер

Вопрос 6 Что обеспечивает электронная подпись при корректном применении?

- А) Подтверждение авторства и контроль целостности подписанных данных
- Б) Физическую защиту помещения
- В) Увеличение объема памяти
- Г) Маскирование сетевого адреса

Вопрос 7 Какой компонент обычно используется для фильтрации сетевого трафика по заданным правилам?

- А) Межсетевой экран
- Б) Текстовый редактор
- В) Архиватор
- Г) Драйвер принтера

Вопрос 8 Для чего применяются программно-аппаратные средства доверенной загрузки?

- А) Для контроля целостности и допустимости компонентов, запускаемых при загрузке системы
- Б) Для увеличения яркости монитора
- В) Для очистки временных файлов
- Г) Для сжатия сетевого трафика

Вопрос 9 Что следует делать при изменении состава автоматизированной системы или выявлении новых угроз?

- А) Пересмотреть применяемые меры и настройки средств защиты
- Б) Отключить журналирование
- В) Удалить все политики доступа
- Г) Предоставить пользователям административные права

Вопрос 10 Что характеризует комплексный подход к защите автоматизированной системы?

- А) Совместное применение программных, программно-аппаратных, криптографических и организационных мер
- Б) Использование только одного антивируса
- В) Применение только паролей

Г) Отказ от технических средств защиты

Критерии оценки:

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания при тестировании

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%

**ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ
ДОПОЛНИТЕЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ
ПЕРЕПОДГОТОВКИ**

Сетевые системы и защита данных

Вид профессиональной деятельности: Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности

Трудоемкость: 1286 часов

Срок обучения: 80 недель

Форма обучения: Очно-заочная с применением ДОТ

Режим занятий: 17 часов в неделю

Москва, 2026

1. Общие положения

Программа итоговой аттестации дополнительной профессиональной программы «Сетевые системы и защита данных» в сфере деятельности: обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности, разработана на основе Порядка проведения Итоговой аттестации по дополнительным профессиональным программам.

Итоговая аттестация представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы. Итоговая аттестация проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

Итоговая аттестация является обязательной для слушателей, завершающих обучение по дополнительной профессиональной программе профессиональной переподготовки.

К итоговой аттестации допускается слушатель, не имеющий задолженности и в полном объеме выполнивший учебный план по ДПП.

Итоговая аттестация слушателей проводится с целью установления соответствия достигнутых результатов освоения ДПП заявленным целям и запланированным результатом обучения.

Итоговая аттестация по программе профессиональной переподготовки проводится в форме итогового экзамена (в том числе в форме тестирования). Видом итоговой аттестации выпускников по ДПП программе профессиональной переподготовки «Сетевые системы и защита данных» в сфере деятельности: обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности.

При применении итоговых аттестационных испытаний с применением электронного обучения, дистанционных образовательных технологий обеспечивается идентификация личности слушателя и контроль соблюдения установленных учебным планом и настоящим положением норм и требований.

Слушателям, не прошедшим итоговую аттестацию или прервавшим обучение по уважительным причинам (по медицинским показаниям, подтвержденным соответствующими документами), предоставляется возможность переноса срока прохождения итоговой аттестации на основе личного заявления. В случае если слушатель был направлен на обучение организацией, данный вопрос согласовывается с данной организацией.

2. Виды и задачи профессиональной деятельности выпускников

Виды и задачи профессиональной деятельности выпускников, заявленные в программе Сетевые системы и защита данных.

Вид трудовой деятельности - обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности. Уровень квалификации – пятый (Приказ Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта «06.032 Специалист по

безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н и федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427 в рамках общих трудовых функций «Техническое обслуживание средств защиты информации в компьютерных системах и сетях».

Возможное место работы (типы предприятий): коммерческие и некоммерческие организации.

Задачи профессиональной переподготовки: совершенствование имеющихся и формирование новых компетенций у обучающихся для выполнения трудовых функций: А/01.5; А/02.5; А/03.5.

Трудовые функции по Квалификационному справочнику ЕКСД (приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н) «Специалист по безопасности компьютерных систем и сетей»:

- Техническое обслуживание программно-аппаратных средств защиты информации в операционных системах
- Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях
- Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения

3. Требования к результатам освоения программы для выполнения профессиональных (трудовых) функций

Результатом освоения дополнительной профессиональной программы является развитие общекультурных, общепрофессиональных и формирование профессиональных компетенций. В частности, совершенствование имеющихся компетенций:

- ОПК-ИБ-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
- ОПК-ИБ-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
- ОПК-ИБ-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях
- ОПК-ИБ-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям
- ОПК-ИБ-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями
- ОПК-ИБ-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного

назначения, в том числе отечественного производства, для решения задач профессиональной деятельности

- ОПК-ИБ-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности
- ОПК-ИБ-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности
- ОПК-ИБ-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
- ОПК-ИБ-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России и ФСТЭК России
- ОПК-ИБ-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности
- ОПК-ИБ-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
- ОПК-ИБ-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
- ОПК-ИБ-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
- ОПК-ИБ-11 Способен проводить эксперименты по заданной методике и обработку их результатов
- ОПК-ИБ-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

4. Требования к выпускнику, проверяемые в ходе итогового аттестации

Итоговая аттестация предполагает проверку результатов освоения программы профессиональной переподготовки, т.е. оценку сформированности всех компетенций, предусмотренных программой.

Аттестация по ДПП «Сетевые системы и защита данных» осуществляется в форме тестирования.

К итоговой аттестации допускаются обучающиеся, выполнившие учебный план в полном объеме, не имеющие академическую задолженность (задолженность по текущей и промежуточной аттестации).

При прохождении итоговой аттестации выпускники должны показать свою способность и умение, опираясь на полученные знания, сформированные умения, профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности.

Оценка выставляется в соответствии с критериями, приведенными в п. 8 настоящей программы по принятой двух балльной системе. По окончании заседания результаты объявляются Председателем аттестационной комиссии.

По результатам аттестационных испытаний обучающийся имеет право на апелляцию.

5. Порядок формирования и состав аттестационной комиссии

Итоговая аттестационная комиссия создаётся в целях комплексной оценки уровня знаний слушателей с учетом целей обучения, вида ДПП, установленных требований к содержанию ДПП, результатов промежуточных испытаний.

Аттестационную комиссию возглавляет председатель, который организует и контролирует ее деятельность, обеспечивает единство требований, предъявляемых к слушателям. Председателем аттестационной комиссии по программе профессиональной переподготовки целесообразно определять лицо, не работающее в образовательной организации, как правило, из числа ведущих специалистов предприятий, организаций и учреждений, по профилю осваиваемой слушателями программы.

Аттестационная комиссия формируется из преподавателей университета, лиц, приглашенных из сторонних организаций и учреждений: преподавателей других учреждений и специалистов предприятий и организаций по профилю осваиваемой слушателем программы.

Дата и время проведения заседания итоговой аттестационной комиссии по ДПП профессиональной переподготовки устанавливается ректором АНО ВО «Университет ИТ ХАБ» и доводится до сведения всех членов аттестационной комиссии за 14 (четырнадцать) календарных дней до начала итогового испытания.

При устной форме итоговых испытаний решение аттестационной комиссией принимается на закрытых заседаниях простым большинством голосов членов комиссий, участвующих в заседании. При равном числе голосов голос председателя является решающим. Решение комиссий принимается непосредственно на заседании после оформления и подписания протокола, и сообщается слушателю.

Результаты итоговой аттестации слушателей ДПП фиксируются в соответствующих документах, определяемых настоящим Положением, и хранятся в архиве АНО ВО «Университет ИТ ХАБ» согласно номенклатуре дел.

Решение по результатам проведения итоговой аттестации слушателей по ДПП профессиональной переподготовки оформляется следующими документами:

- протокол заседания аттестационной комиссии по результатам итогового тестирования;

- отчет о работе аттестационной комиссии (ежеквартальный).

6. Порядок подготовки и проведения итоговой аттестации

Итоговая аттестация проводится в форме Тестирования.

Тестирование может проводиться в аудитории или с использованием электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ) на базе университетской информационной платформы (LMS).

К прохождению итогового тестирования допускаются обучающиеся, выполнившие все виды учебной работы, предусмотренные рабочей программой дисциплины, и имеющие положительную оценку по текущему контролю.

Продолжительность итогового тестирования составляет 60 минут. Тестовые задания разрабатываются в соответствии с фондом оценочных средств и охватывают все тематические разделы дисциплины.

Во время проведения тестирования обучающимся запрещается пользоваться посторонними источниками информации (учебниками, конспектами, мобильными телефонами и другими электронными устройствами), если иное прямо не предусмотрено условиями проведения теста. Нарушение правил академической честности влечет за собой аннулирование результатов тестирования.

Итоговая оценка формируется на основе результатов автоматизированной или экспертной проверки тестовых заданий. Оценка выставляется путем подсчета количества правильных ответов и перевода полученного первичного балла в шкалу оценивания, установленную локальными нормативными актами вуза.

Основными оцениваемыми показателями (индикаторами достижения компетенций) при итоговом тестировании являются:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

7. Перечень рекомендуемой литературы

1. Аман, К. П. Компьютерные сети : учебное пособие / К. П. Аман, А. А. Мусина. — Алма-ты, Москва : EDP Hub (Идипи Хаб), Ай Пи Ар Медиа, 2025. — 251 с. — ISBN 978-5-4497-4131-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/148113.html>
2. Солоневич, А. В. Компьютерные сети : учебник / А. В. Солоневич. — Минск : Республиканский институт профессионального образования (РИПО), 2021. — 208 с. — ISBN 978-985-7253-43-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/134078.html>

3. Гулевич, Д. С. Сети связи следующего поколения : учебное пособие / Д. С. Гулевич. — 3-е изд. — Москва : Интернет- Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 212 с. — ISBN 978-5-4497-0933-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/102063.html>
4. Сергеев М.Ю. Компьютерные сети : практикум / Сергеев М.Ю., Сергеева Т.И., Олейникова С.А.. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2019. — 154 с. — ISBN 978-5-7731-0739-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/93261.html>

Информационно-библиотечные ресурсы (ссылки на информационные ресурсы АНО ВО «Университет ИТ ХАБ»):

№	Наименование портала (ресурса)	Ссылка
1.	Образовательная платформа Юрайт. Для вузов и ссузов	https://urait.ru/

8. Критерии оценки результатов обучения членами аттестационной комиссии

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух балльной шкале («зачтено\незачтено»). Результаты итоговой аттестации заносятся в соответствующие документы.

Результаты освоения программ профессиональной переподготовки оцениваются по двух балльной шкале в соответствии с нижеприведенными критериями:

Оценка	Критерии выставления оценки
Зачтено	Количество верных ответов в интервале: 71-100%
Не зачтено	Количество верных ответов в интервале: 0-70%