Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Донецкий филиал РАНХиГС

УТВЕРЖДАЮ
Директор института - филиала
Л.Б. Костровец

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 009C34BED1E8FD26E5229ECE1020F38E62
Владелец: Костровец Лариса Борисовна
Действителен: с 30.03.2026 до 23.06.2027

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Информационная безопасность»

(наименование программы)

Донецк, 2026

Разработчики:

Доцент кафедры информационных технологий
Донецкого филиала РАНХиГС,
кандидат технических наук, доцент _____ И.Л. Семичастный
(подпись)

Заместитель директора центра дополнительного
профессионального образования
Донецкого филиала РАНХиГС _____ Е.А. Шумкова
(подпись)

Руководитель программы:

Начальник отдела повышения квалификации
специалистов центра дополнительного профессионального
образования Донецкого филиала РАНХиГС _____ В.Л. Савченко
(подпись)

Дополнительная профессиональная программа повышения квалификации рассмотрена на заседании ученого совета Донецкого филиала РАНХиГС и рекомендована к реализации, протокол № 7 от «14» апреля 2026 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель и задачи реализации программы

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» разработана для повышения эффективности профессиональной служебной деятельности лиц, замещающих должности в органах публичной власти, руководителей и сотрудников подведомственных организаций Донецкой Народной Республики в сфере обеспечения информационной безопасности, в соответствии с распоряжением Правительства Российской Федерации от 21 апреля 2023 года № 1019-р и поручением Президента Российской Федерации (Пр-2180 от 16.11.2022) в целях создания условий для кадрового обеспечения достижения национальных целей развития Российской Федерации и реализации мероприятий программы социально-экономического развития Донецкой Народной Республики, Луганской Народной Республики, Запорожской и Херсонской областей.

Программа актуальна и своевременна, так как в условиях цифровой трансформации и активного использования информационных технологий защита информации становится особенно важной. Программа направлена на формирование у слушателей профессиональных компетенций, повышение профессионального уровня в обеспечении информационной безопасности.

В программе рассматриваются основные вопросы организационно-правового и методического обеспечения технической защиты информации в Российской Федерации, каналы утечки информации ограниченного доступа на объектах информатизации, меры и средства защиты, методы обеспечения безопасности персональных данных, технологии обеспечения информационной безопасности, противодействия киберугрозам и социальным атакам, информационная безопасность при работе с ЭДО и государственными услугами, а также практические аспекты обеспечения информационной безопасности в условиях деятельности органов власти.

Целью реализации программы является формирование и совершенствование компетенций специалистов органов государственной и муниципальной власти в области защиты информации, обеспечения безопасности персональных данных, противодействия киберугрозам и выполнения требований регуляторов (ФСТЭК, ФСБ, РКН).

Задачами реализации программы являются:

- ознакомление слушателей с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, нормативными правовыми и организационными основами обеспечения безопасности персональных данных в информационных системах персональных данных;
- ознакомление с практическими аспектами обеспечения информационной безопасности в условиях деятельности органов власти;
- ознакомление слушателей с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, нормативными правовыми и организационными основами обеспечения безопасности персональных данных в информационных системах персональных данных;
- формирование умений выбора решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах;

- изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценка степени их опасности;

- оказание помощи организациям и учреждениям в повышении квалификации сотрудников, в чьи должностные обязанности входит обеспечение защиты информации.

1.2. Нормативная правовая база

Дополнительная профессиональная программа повышения квалификации разработана на основании следующих нормативных правовых документов:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изм. и доп. от 29.12.2025 г.).
2. Постановление Правительства РФ от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».
3. Приказ Министерства науки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрировано в Минюсте России 22.04.2025 № 81928).
4. Приказ Минобрнауки России от 12.09.2013 № 1061 (ред. от 13.12.2021) «Об утверждении перечней специальностей и направлений подготовки высшего образования» (зарегистрировано в Минюсте России 14.10.2013 № 30163).
5. Приказ Минобрнауки России от 13.08.2020 № 1016 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление».
6. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства науки и высшего образования РФ от 17 ноября 2020 г. № 1427 (зарегистрирован в Минюсте РФ 18 февраля 2021 г. № 62548).
7. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. № 525н (зарегистрирован Министерством юстиции Российской Федерации 28 октября 2022 г., регистрационный № 70543).
8. Приказ РАНХиГС от 02 декабря 2025 г. № 02-02669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ – программ повышения квалификации, программ профессиональной переподготовки.
9. Приказ РАНХиГС от 22 сентября 2017 г. № 01-6230 «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».
10. Методические рекомендации-разъяснения по разработке дополнительных профессиональных программ на основе профессиональных стандартов (утв. Минобрнауки России 22.04.2015 № ВК-1032/06).
11. Нормативные документы, определяющие требования к выпускнику программы:

– «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (с изм. от 28.12.2024);

– ОК 016-2025 Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР) (утв. Приказом Росстандарта от 16.05.2025 № 423-ст);

– «ЕКС - Единый классификационный справочник должностей руководителей, специалистов и других служащих, установленный постановлением Правительства РФ от 31.10.2002 № 787;

– Квалификационный справочник. Должностей руководителей, специалистов и других служащих, утвержденный Постановлением Минтруда РФ от 21 августа 1998 г. № 37;

– «Справочник квалификационных требований к специальностям, направлениям подготовки, знаниям и умениям, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих» (утв. Минтрудом России) https://www.consultant.ru/document/cons_doc_LAW_219036/.

1.3. Планируемые результаты обучения

Таблица 1.1

Перечень профессиональных компетенций в рамках имеющейся квалификации и профессиональных компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, СК) *(формируются и (или) совершенствуются)*	Практический опыт	Знания	Умения
1	2	3	4	5
ВД 1. Работа с информацией в современном обществе	ОПК-1[1]. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Владеть: - навыками выявления базовых угроз информационной безопасности (подозрительные письма, нестандартное поведение ПО) и применения инструкций по режиму защиты информации на рабочем месте; - навыками использования программных и аппаратных средств защиты информации (антивирусы, СКЗИ,	Знать: - базовый понятийный аппарат в области информационной безопасности; - виды угроз информационным системам, а также методы, технологии обеспечения информационной безопасности; - принципы обеспечения конфиденциальности, целостности и доступности информации; - основные виды угроз (естественные,	Уметь: - идентифицировать базовые угрозы для рабочего места и организации; - различать грифы и пометки конфиденциальности во входящих документах; - применять инструкции по режиму секретности и конфиденциальности на рабочем месте; - использовать современные программные и

[1] Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства науки и высшего образования РФ от 17 ноября 2020 г. № 1427 (зарегистрирован в Минюсте РФ 18 февраля 2021 г. № 62548)

		блокировка экрана) для обеспечения конфиденциальности, целостности и доступности информации на рабочем месте	техногенные, антропогенные); - понятия уязвимости, риска, источника угрозы	аппаратные средства для защиты информации на рабочем месте
ВД 2. Работа с нормативными правовыми актами по защите информации в сфере профессиональ-ной деятельности	ОПК-5[1]. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Владеть: - навыками поиска актуальных нормативных правовых актов (Конституция РФ, федеральные законы, приказы регуляторов) в справочно-правовых системах и на официальных сайтах органов власти; - навыками использования требований 149-ФЗ, 152-ФЗ, 187-ФЗ при организации технологического процесса защиты информации и решении практических задач на рабочем месте	Знать: - иерархию нормативных правовых актов в сфере ИБ (Конституция РФ, федеральные законы, подзаконные акты, приказы регуляторов)	Уметь: - применять требования 149-ФЗ, 152-ФЗ, 187-ФЗ в повседневной деятельности
ВД-3. Обработка и защита персональных данных	ПСК-1[2]. Способен организовать обработку и защиту персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ и подзаконных актов	Владеть: - навыками обеспечения установленных законодательством процедур обработки ПДн: от классификации информации и получения согласия до обезличивания (деперсонификации) и уничтожения данных по истечении сроков хранения или по требованию субъекта; - навыками идентификации типовых каналов утечки конфиденциальной информации (бумажные и электронные носители, мессенджеры) и применения превентивных мер	Знать: - понятие конфиденциальной информации, персональных данных, служебной тайны, а также понятие «открытая информация»; - правовой режим персональных данных (ПДн); - категории ПДн; - обязанности оператора; - правила деперсонификации и обезличивания; - порядок получения и отзыва согласия на обработку ПДн; - требования к трансграничной передаче и локализации данных; - типовые каналы утечки ПДн (бумажные носители, электронная почта, съемные диски, мессенджеры)	Уметь: - разрабатывать локальные акты об обработке ПДн; - получать согласие на обработку ПДн; - обеспечивать уничтожение ПДн по требованию субъекта или по истечении срока хранения; - оформлять уведомления в Роскомнадзор; - классифицировать информацию, содержащую ПДн; - применять средства DLP-систем (в части уведомления о попытках отправки)

[2] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. № 525н (зарегистрирован Министерством юстиции Российской Федерации 28 октября 2022 г., регистрационный № 70543), (трудовая функция В/08.6, В/09.6, В/10.6).

ВД-4. Работа с программно-аппаратными и криптографическими средствами защиты информации	ПСК-2[2]. Способен применять программно-аппаратные и криптографические средства защиты информации в повседневной деятельности	Владеть: - навыками настройки и поддержания антивирусной защиты (обновление сигнатур, сканирование узлов и съемных носителей), а также корректного использования межсетевых экранов и систем обнаружения вторжений; - навыками использования СКЗИ (например, КриптоПро CSP, VipNet) для организации защищенных каналов связи, шифрования данных и обеспечения безопасного электронного документооборота; - навыками проверки сертификатов ключей проверки электронной подписи, а также корректного применения ЭП при подписании и шифровании документов	Знать: - принципы работы антивирусных средств, межсетевых экранов, систем обнаружения вторжений; - основы применения средств криптографической защиты информации (СКЗИ), включая КриптоПро CSP и VipNet; - правила работы с электронной подписью (ЭП)	Уметь: - настраивать антивирусную защиту; - использовать СКЗИ для шифрования каналов связи и ЭДО; - проверять сертификаты ключей проверки ЭП
ВД-5. Использование в профессиональной деятельности информационно-коммуникационных технологий	ОПК-5[3]. Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг	Владеть: - навыками работы с универсальными пакетами прикладных программ для решения управленческих задач, использования систем управления базами данных для организации, хранения, поиска и обработки информации; - навыками работы со средствами защиты информации, формальной постановки и решения задачи обеспечения информационной безопасности;	Знать: - требования нормативных правовых актов в области защиты государственной тайны и конфиденциальной информации при работе в государственных информационных системах (ГИС); - основные требования ФСТЭК и ФСБ к защите ГИС; - правила работы с конфиденциальными документами; - государственные и муниципальные информационные системы технологии электронного правительства и предоставления государственных (муниципальных) услуг;	Уметь: - анализировать крупные массивы данных с использованием современных программных средств; - применять инструменты цифровой культуры в принятии организационно-управленческих решений; - осуществлять выбор информационной системы для обработки информации; - организовывать поиск информации для решения задач государственного и муниципального управления;

[3] Федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению 38.03.04 Государственное и муниципальное управление, утвержденный приказом Министерства науки и высшего образования Российской Федерации от 13 августа 2020 г. № 1016 (зарегистрирован в Минюсте России 27 августа 2020 г. № 59497)

		- основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации	- основные программные средства государственных и муниципальных информационных систем и сфера их применения в области профессиональных задач; - тенденции и перспективы развития и использования информационно-коммуникационных технологий в профессиональной деятельности	- управлять основными информационно-коммуникационными технологиями; - применять технологии электронного правительства и предоставления государственных (муниципальных) услуг; - использовать навыки работы с законами и иными нормативно-правовыми актами, регламентирующими порядок и организацию предоставления государственных и муниципальных услуг
ВД-6. Противодействие киберугрозам и социальным атакам	ПСК-3[2]. Способен выявлять и противодействовать атакам с использованием методов социальной инженерии (фишинг, вишинг, смишинг), а также участвовать в реагировании на инциденты информационной безопасности	Владеть: - навыками выявления признаков фишинговых писем (проверка URL, адреса отправителя), вишинга (звонки от «службы безопасности») и смишинга, а также навыками безопасного завершения подозрительных контактов и использования мессенджеров; - навыками оперативной блокировки доступа при компрометации учетной записи или заражении вредоносным ПО, фиксации фактов инцидентов для служебного расследования и взаимодействия с подразделением ИБ (включая информирование о подозрительных активностях и взаимодействие с ГосСОПКА)	Знать: - признаки фишинговых писем и подозрительных звонков; - способы противодействий киберугрозам и социальным атакам; - методы телефонного мошенничества и защиты от спама; правила безопасного использования мессенджеров и социальных сетей; - методы вишинга (звонки от «службы безопасности»); - порядок действий при компрометации учетной записи или заражении вредоносным ПО; - порядок взаимодействия с ГосСОПКА; - риски использования личных устройств; правила создания надежных паролей; принципы двухфакторной аутентификации	Уметь: распознавать фишинговые атаки; - не переходить по подозрительным ссылкам; - применять двухфакторную аутентификацию; оперативно блокировать доступ при инцидентах; фиксировать факты инцидентов для служебного расследования; - проверять URL перед переходом; - завершать подозрительные звонки; - сообщать о подозрительных активностях в ИБ-отдел
ВД-7. Работах в системах электронного документооборота (СЭД)	ПСК-4[2]. Способен безопасно работать в системах электронного документооборота (СЭД) и на Едином портале государственных и муниципальных услуг (ЕПГУ), обеспечивая сохранность учетных данных и ключей ЭП	Владеть: - навыками распознавания фишинговых страниц Госуслуг и иных поддельных ресурсов, использования подтвержденной учетной записи только на официальных сайтах, своевременной	Знать: - способы информационной безопасности при работе с ЭДО и государственными услугами; - типовые схемы мошенничества с аккаунтами Госуслуг; - правила	Уметь: - распознавать попытки перехвата учетной записи через фишинговые страницы Госуслуг; - использовать подтвержденную учетную запись только на официальных

		смены паролей и применения правил подтверждения входа в ЕСИА; - навыками оперативной блокировки доступа к учетной записи и подачи заявления на отзыв сертификата ключа проверки электронной подписи в случае утери носителя или компрометации пароля в соответствии с установленным порядком	подтверждения входа в ЕСИА; - сроки действия сертификатов ЭП; - порядок действий при утере носителя (Рутокен/флешка) с ключом ЭП или компрометации пароля	ресурсах; - своевременно менять пароли доступа к ЕСИА; - оперативно блокировать доступ; - подавать заявление на отзыв сертификата ключа проверки ЭП

1.4. Категория слушателей

Программа предназначена для лиц, замещающих должности в органах публичной власти, руководителей и сотрудников подведомственных организаций Донецкой Народной Республики.

Требования к уровню профессионального образования: среднее профессиональное образование, высшее образование (бакалавриат, магистратура, специалитет).

1.5. Формы обучения и сроки освоения

Форма обучения – очная (с применением электронного обучения и дистанционных образовательных технологий).

Общая трудоемкость программы – 36 академических часов, из которых 24 академических часа контактной работы со слушателем, в том числе 12 академических часов с применением дистанционных образовательных технологий, 2 академических часа итоговой аттестации, 10 академ. часов – самостоятельная работа.

1.6. Период обучения и режим занятий

Периоды обучения составляют: 1 неделя, 5 дней (см. табл.2.1).

Режим занятий: 5-6 дней в неделю, 4-8 академических часов в день.

Предельная максимальная численность лекционной группы – 100 человек, практической (семинарской) группы – 40 человек.

1.7. Документ о квалификации

Удостоверение о повышении квалификации федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации».

2. СОДЕРЖАНИЕ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

2.1. Календарный учебный график

Таблица 2.1

Календарный учебный график

Период обучения – 1 неделя, 5 дней	
1 неделя	**5 дней**
УЗ/УЗ ДОТ /СР ЭО	УЗ ДОТ/ СР ЭО/ИА ДОТ

Календарный учебный график выполнен с помощью следующих условных обозначений:
УЗ – учебные занятия;
УЗ ДОТ– учебные занятия с применением дистанционных образовательных технологий;
СР ЭО – самостоятельная работа с применением электронного обучения;
ИА ДОТ – итоговая аттестация с применением дистанционных образовательных технологий.

Таблица 2.2

2.2. Учебный план

Учебный план
по дополнительной профессиональной программе повышения квалификации
«Информационная безопасность»

№ п/п	Наименование темы	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.					Самостоятельная работа (в т.ч. электронное обучение), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции / в интерактивной форме	Практические (семинарские) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.	Введение в информационную безопасность	4	2	2										2			З(Д)	ОПК-1[1] ОПК-5[1]
2.	Информационная безопасность и персональные данные	6	4		4									2			З(Д)	ПСК-1[2]
3.	Технологии обеспечения информационной безопасности	6	4		4									2			З(Д)	ПСК-2[2]
4.	Защита информации в органах государственной власти	6	2	2					2	2				2			З(Д)	ОПК-5[3]
5.	Противодействие киберугрозам и социальным атакам	6							4	2	2			2			З(Д)	ПСК-3[2]
6.	Информационная безопасность при работе с ЭДО и госуслугами	4							4	2	2						З(Д)	ПСК-4[2]
7.	Инструкция по обеспечению информационной безопасности для организаций	2							2	2							З(Д)	ПСК-1[2] ПСК-2[2] ПСК-3[2]
	Итого:	**34**	**12**	**4**	**8**				**12**	**8**	**4**			**10**				
	Итоговая аттестация:	**2**	**тестирование**														**З/2**	
	Всего:	**36**	**12**	**4**	**8**				**12**	**8**	**4**			**10**			**2**	

З(Д) - зачет (с применением дистанционных образовательных технологий)

2.3. Содержание программы по темам

Таблица 2.3

Содержание программы по темам

Номер темы и её наименование	Содержание темы
Тема 1. Введение в информационную безопасность	Введение в информационную безопасность. Основные угрозы информационной безопасности; нормативно-правовое регулирование ИБ в РФ; роль госслужащего в обеспечении ИБ
Тема 2. Информационная безопасность и персональные данные	Федеральный закон № 152-ФЗ; обработка и защита персональных данных; ответственность за нарушения. Изменения в Законе. Особенности работы с биометрическими данными
Тема 3. Технологии обеспечения информационной безопасности	Правила создания паролей. Системы KeyPass, LastPass. Криптография. Классификация методов криптографии. Антивирусные средства
Тема 4. Защита информации в органах государственной власти	Основные требования к защите информации. Государственная тайна, служебная информация ограниченного доступа. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений
Тема 5. Противодействие киберугрозам и социальным атакам	Противодействие киберугрозам и социальным атакам. Рекомендации по противодействию фишингу, социальным атакам, социальному инжинирингу
Тема 6. Информационная безопасность при работе с ЭДО и госуслугами	Работа с ЭДО. Работа с госуслугами
Тема 7. Инструкция для организаций по информационной безопасности	Обзор инструкции для организаций по информационной безопасности

3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое и программное обеспечение реализации программы

Донецкий филиал РАНХиГС располагает необходимой материально-технической базой, обеспечивающей реализацию программы повышения квалификации, проведение итоговой аттестации, предусмотренной учебным планом.

Очные занятия программы осуществляются в оборудованных аудиториях с возможностью использования преподавателем мультимедийного проектора, ноутбука или стационарного компьютера, средств звуковоспроизведения, экрана, флипчарта, обычной или

электронной доски, доступа к беспроводным сетям Wi-Fi с выходом в Интернет для проведения занятий лекционно-практического типа; практические занятия проводятся в компьютерном классе, а также имеются помещения для самостоятельной работы.

Программное обеспечение: лицензионные системные программы - операционные системы (Windows, Acrobat Reader, иные), обеспечивающие взаимодействие всех других программ с оборудованием и взаимодействие пользователя персонального компьютера с программами; универсальные офисные прикладные программы и средства ИКТ, например: программа подготовки презентаций; свободный доступ каждого слушателя и научно-педагогического работника к средствам информационных и коммуникационных технологий, использованию Интернета, электронной почты, автоматизированных поисковых систем Интернет (например, Yandex).

Во время обучения слушатели имеют доступ к библиотечному фонду с необходимым количеством учебной, методической литературы и другой печатной продукции, для самостоятельной работы, а также к автоматизированным системам хранения и поиска информации, национальным и международным информационным ресурсам.

В программе частично используются электронное обучение и дистанционные образовательные технологии. Электронное обучение связано с прохождением электронного курса. Дистанционное обучение включает в себя изучение материалов. Онлайн занятия реализуются в форме вебинаров, которые проводятся в режиме видеоконференции на платформе МТС Линк.

Слушателям предоставляется авторизованный доступ на информационно-образовательный портал ВШГУ через ввод логина и пароля. Логин и пароль присваивается администратором системы дистанционного обучения. Портал включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающую освоение слушателями образовательных программ полностью или частично независимо от их места нахождения.

Слушателям предоставляется расписание занятий, дополнительный курс, методические материалы для прохождения обучения. Итоговая аттестация проходит в форме онлайн тестирования на информационно-образовательном портале ВШГУ.

Адрес электронного размещения платформы: https://portal.gosedu.ru.

Слушатели получают методическую поддержку в процессе обучения и по завершении обучения, в т.ч. имеют возможность получать консультации по электронной почте у преподавателей, принимающих участие в обучении.

3.2. Учебно-методическое и информационное обеспечение программы

Самостоятельная работа

1. В ходе изучения представленных тем необходимо провести анализ актуальных редакций профильных федеральных законов и подзаконных актов, уделив особое внимание изменениям. Слушатели самостоятельно изучают материалы законов (табл.3.1)

Таблица 3.1

Самостоятельная работа слушателя

Номер темы и её наименование	Содержание самостоятельной работы
Тема 1. Введение в информационную безопасность	Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» https://www.consultant.ru/document/cons_doc_LAW_61798/
Тема 2. Информационная безопасность и персональные данные	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» https://www.consultant.ru/document/cons_doc_LAW_61801/, в том числе положений, вступивших в силу в 2025 году
Тема 3. Защита информации в органах государственной власти	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (последняя редакция) https://www.consultant.ru/document/cons_doc_LAW_220885/ **Приказ Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»** https://normativ.kontur.ru/document?moduleId=1&documentId=500478

Примерные задания для проведения практических занятий

Тема 2. Информационная безопасность и персональные данные

Практическая работа 1. Вопросы для обсуждения:

1. Зачем необходимо принимать меры по защите персональных данных?
2. Что такое персональные данные? Из каких трех блоков они состоят?
3. Чем принципиально отличаются общие, специальные и биометрические персональные данные?
4. Как согласно 152-ФЗ можно обрабатывать специальные и биометрические данные гражданина?
5. Кого касаются правила обработки персональных данных?
6. Распространяется ли 152-ФЗ только на сотрудников организации либо он касается данных кандидатов и уволенных сотрудников?
7. Кто несет ответственность в случае нарушений 152-ФЗ?
8. В каких случаях нужно получать согласие на обработку ПД соискателя должности?
9. Кто такой оператор ПД? С какого момента организация становится оператором ПД?
10. Как организации следует оформлять согласие сотрудника на обработку ПД?

Практическая работа 2. Вопросы для обсуждения:

1. Разъясните, что такое обезличенные ПД?
2. Как можно обрабатывать обезличенные ПД, разъясните?
3. Разъясните, что такое «состав обезличенных данных» согласно новой статье 13.1 152-ФЗ?
4. Объясните, какие права получило Министерство цифрового развития (Минцифры) по поводу ПД для загрузки их в федеральную ГИС в обезличенном виде?
5. Может ли гражданин запретить передачу его обезличенных данных в ГИС?
6. Могут ли городские камеры наблюдения и аудиосенсоры собирать и анализировать обезличенную информацию (например, подсчитывать поток людей, фиксировать события) без нарушения 152-ФЗ?
7. Разъясните, в чем заключается контроль над данной операцией?
8. Объясните, что означает Метод введения идентификаторов?
9. Разъясните, что означает Метод декомпозиции (разбиения)?
10. Разъясните, что означает Метод перемешивания (шуффлинг)?

Тема 3. Технологии обеспечения информационной безопасности

Практическая работа 1. Вопросы для обсуждения:

1. Изучите требования по созданию надежных паролей.
2. Скачайте программу генерации паролей Advanced Password Generator по ссылке https://drive.google.com/open?id=1Q7qLTrCefuZNJ3XDzq0FFZ2lWIsINW-S.
3. Сгенерируйте при помощи скачанной программы группы паролей по следующей схеме: 8-9(10)-12-20 символов (буквы / буквы+цифры / буквы+цифры+спецсимволы).
4. При помощи интернет-ресурсов https://www.passwordmonster.com/ и https://bitwarden.com/password-strength/ проверьте сгенерированные пароли. Опишите изменения стойкости паролей в зависимости от их структуры (описания подтвердите скриншотами). Являются ли они надежными?
5. Создайте на основе изученных Вами правил надежный пароль уровня Strong. Запишите его и используйте в своей работе.
6. Ознакомьтесь с программным продуктом хранения паролей KeePass, скачав его с интернет-ресурса https://keepass.info/.
7. Для знакомства с работой программы скачайте программу, установите программу KeePass и создайте свою базу данных паролей.
8. Создайте свою портативную базу на сменном носителе.
9. Создайте новую базу паролей. Добавьте записи о пароле в базу. Добавьте в свою базу все пароли: для почты, соцсетей и другие пароли.
10. Ознакомьтесь с работой генератора паролей. Воспользуйтесь генератором для создания мастер-пароля.
11. Создание резервной копии базы. Создать резервную базу паролей.
12. Все результаты подтвердите скриншотами.
13. Ознакомьтесь с работой сервиса хранения паролей LastPass https://www.lastpass.com/ru. Опишите его сильные и слабые стороны, обоснуйте свои выводы.
14. Для сервиса LastPass повторите пункты с 6 по 10.

15. Все результаты подтвердите скриншотами, для чего создайте презентацию вашей работы.

Практическая работа 2. Вопросы для обсуждения:

1. На основании данных варианта задания из Таблицы 1 скачать инсталляционную версию антивирусного пакета.

2. Установить ее на свой ПК, предварительно отключив антивирусный пакет, установленный на нем.

3. Протестировать установленный антивирусный пакет в течение нескольких дней. Изучить режимы его работы, на основании полученных данных заполнить Таблицу № 2 для своего антивирусного пакета по своему варианту. Проверить флешку с его помощью.

4. Сохранить в файле отчета скриншоты основных режимов использования программы-антивируса в формате презентации.

Таблица 3.2

Номер варианта	**Вендор**	**Web-сайт**	**Free-antivirus-download**
1.	Bitdefender	https://bitdefender-antivirus-free.en.softonic.com/download	
2.	Kaspersky	https://www.kaspersky.ru/downloads/free-antivirus?ysclid=m0iizlg0i4963699299 https://www.kaspersky.ru/free-antivirus?ysclid=m0ij3h8nfs660745231	
3.	ESET	https://pro32.com/ru/home/pro32-antivirus/	
4.	Microsoft	https://microsoft-defender.ru.uptodown.com/windows#google_vignette	
5.	Avast	https://www.avast.com/free-antivirus-download#pc	
6.	Norton	https://nortonsecurity.ru/download/	
7.	Avira	https://install.avira-update.com/package/antivirus/win/ru-ru/avira_antivirus_ru-ru.exe	
8.	F-Secure	https://www.f-secure.com/en/try-for-free	
9.	McAfee	https://www.mcafee.com/ru-ru/antivirus/free.html month	
10.	AVG	https://www.avg.com/ru-ru/homepage#pc	
11.	Malwarebytes	https://www.malwarebytes.com/mwb-download	

12.	Trend Micro	https://www.trendmicro.com/ru_ru/forHome/products/free-tools.html	
13.	Sophos	https://www.sophos.com/en-us/products/free-trials	
14.	G Data	https://www.gdata-software.com/downloads	
15.	Panda	https://www.pandasecurity.com/en/homeusers/free-antivirus/	
16.	360Total Sequrity	https://www.360totalsecurity.com/ru	
17.	Doctor Web Sequrity Space	https://download.drweb.by/security_space/?ysclid=m2216092ci394503951	
18.	NANO Антивирус	https://www.nanoav.ru/	
19.	F-Secure	https://www.f-secure.com/en/total	
20.	K7	https://www.k7computing.com/in/	
21.	Bitdefender	https://bitdefender-antivirus-free.en.softonic.com/download	
22.	Kaspersky	https://www.kaspersky.ru/downloads/free-antivirus?ysclid=m0iizlg0i4963699299	
23.	ESET	https://pro32.com/ru/home/pro32-antivirus/	
24.	Microsoft	https://microsoft-defender.ru.uptodown.com/windows#google_vig	
25.	Avast	https://www.avast.com/free-antivirus-download#pc	
26.	Avira	https://install.avira-update.com/package/antivirus/win/ru-ru/avira_antivirus_ru-ru.exe	
27.	F-Secure	https://www.f-secure.com/en/try-for-free	
28.	Trend Micro	https://www.trendmicro.com/ru_ru/forHome/products/free-tools.html	
29.	Doctor Web Sequrity Space	https://download.drweb.by/security_space/?ysclid=m2216092ci394503951	
30.	360Total Sequrity	https://www.360totalsecurity.com/ru	

Таблица 3.3

Наличие режимов программного антивирусного комплекса

№	Режим использования	Название пакета	Достоинства	Недостатки
1.	Защита от руткитов и шпионских программ			
2.	Технология DeepScreen			
3.	Режимы Hardened («белый» список приложений»)			
4.	Веб-защита			
5.	Очистка браузеров «Browser Cleanup»			
6.	Проверка обновлений приложений («Software Updater»)			
7.	Безопасность домашней сети (Home Network Security)			
8.	Сканирование HTTPS			
9.	Интеллектуальное сканирование			
10.	SecureDNS			
11.	«Песочница» («Sandbox»)			
12.	Безопасный рабочий стол «SafeZone»			
13.	Автоматический брандмауэр			
14.	Анти-спам			
15.	Удаленное управление компьютером («AccessAnyware»)			
16.	Безопасное удаление документов			

1. При наличии у изучаемого программного комплекса соответствующего режима в третьем столбце Таблицы 2 ставится +.

2. В файле отчета по данной работе можно дополнить данные Таблицы 2 другими характеристиками и описаниями режимов работы изучаемого антивирусного пакета.

3. По каждому режиму изучаемого антивирусного пакета при защите отчета необходимо показать слайд со скриншотом и дать описание его работы.

4. При защите отчета необходимо дать общую оценку изученного антивирусного программного комплекса.

5. При этом общая оценка должна опираться на выявленные в процессе практической работы с пакетом его достоинства и недостатки. Их необходимо сформулировать и отразить в Таблице 2. При этом необходимо выяснить, что представляет собой каждый режим использования.

Тема 5. Противодействие киберугрозам и социальным атакам

Практическая работа 1. Вопросы для обсуждения:

1. Разъясните, что такое социальная инженерия?
2. Объясните, что в условиях информационного общества облегчает кибермошенникам задачу получения доступа к конфиденциальным данным граждан РФ?
3. Разъясните, что такое фишинг?
4. Расскажите, какие разновидности фишинга Вам известны? Опишите эти виды кибермошенничества.
5. Объясните, что такое претекстинг?
6. Опишите такой вид кибермошенничества, как квид про кво?
7. Разъясните, в чем заключается вид мошенничества использование подложных ссылок?
8. Объясните, что означает такой вид мошенничества, как вишинг?
9. Разъясните, что означает технология дип фейков? В чем проявляется ее растущая опасность?
10. Опишите, возможные последствия совершенной кибератаки для Вашей организации.

Практическая работа 2. Вопросы для обсуждения:

1. Разъясните, в чем заключается методологический аспект противодействия кибермошенникам?
2. Объясните, в чем заключается образовательный аспект противодействия кибермошенникам?
3. Разъясните, что такое технология DLP (Data Loss Prevention или Data Leakage Prevention)?
4. Расскажите, какие инструменты использует технология DLP?
5. Сформулируйте, какие четыре аспекта практической деятельности помогают защититься организации изнутри?
6. Опишите, на основании каких двух направлений противодействия мошенникам строится работа по защите организации?
7. Разъясните, в чем заключается поведенческая аналитика сотрудников?
8. Объясните, к чему сводится аудит хранения информации и управление правами доступа к ней?
9. Разъясните, как проверяется посещаемость веб-ресурсов сотрудниками организации?
10. Опишите, на что необходимо обратить внимание при анализе использования сотрудниками ПО?

Тема 6. Информационная безопасность при работе с ЭДО и госуслугами

Практическая работа 1. Вопросы для обсуждения:

1. Объясните, в чем заключается основа технологии ЭДО?
2. Какие преимущества дает ведение документооборота в электронном виде в целом?
3. Перечислите основные функции, которые реализует программный продукт ЭДО?

4. Разъясните, в чем заключается как количественный, так и качественный эффект от внедрения программы ЭДО в организации?

5. Опишите, что такое автоматизация на основе ЭДО в организации?

6. Объясните, в чем конкретно заключаются положительные последствия для организации от внедрения ЭДО?

7. Разъясните, в чем заключаются недостатки от внедрения ЭДО в организации?

8. Опишите, какие организационные и технические мероприятия необходимо выполнить компании, внедряющей ЭДО?

9. Разъясните, как работает ЭДО в процессе эксплуатации, какие процессы работы с документацией выполняет этот программный комплекс и в чем заключается смысл этих операций?

10. Опишите разновидность такой задачи, реализуемой ЭДО как формирование архивов в организации.

11. Опишите разновидность такой задачи, реализуемой ЭДО, как работа со средствами workflow (WF) в организации.

12. Опишите разновидность такой задачи, реализуемой ЭДО, как формирование базы знаний в организации.

13. Опишите разновидность такой задачи, реализуемой ЭДО, как коллаборация (collaboration) в организации.

14. Опишите разновидность такой задачи, реализуемой ЭДО, как создание CRM-системы (Customer relationchip management) в организации.

15. Опишите разновидность такой задачи, реализуемой ЭДО, как организация госзакупок в организации.

16. Объясните, возможно ли совмещение системы ЭДО с обычной (бумажной) формой документации?

17. Объясните, как организуется хранение документов в ЭДО?

18. Сформулируйте общие рекомендации выбора СЭД для внедрения ее в организации.

19. Разъясните, какие сложности необходимо преодолеть компании, внедряющей ЭДО, и в чем заключается основная проблема внедрения.

20. Опишите наиболее известные на рынке РФ и СНГ программные продукты ЭДО.

Практическая работа 2. Как зарегистрироваться на Госуслугах в 2026 году

Сервис Госуслуги может существенно облегчить жизнь любого гражданина, поэтому все-таки стоит создать аккаунт на этом портале. Ведь можно будет оплачивать штрафы, платить налоги или записываться на прием к врачу, не выходя из дома. В материале рассказывается о том, как пройти процедуру регистрации на Госуслугах в 2026 году и получить подтвержденную учетную запись.

Полное название портала — «Единый портал государственных и муниципальных услуг Российской Федерации». Причем работать с ним можно не только с компьютера при помощи десктопного браузера, поскольку существуют приложения для платформ Android и iOS. Поэтому есть возможность зарегистрироваться в Госуслугах даже через телефон.

Нормативно-правовые документы:

1. Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (с изм. и доп. от 08 августа 2024 г.) http://www.consultant.ru/document/cons_doc_LAW_48601/ (дата обращения: 15.03.2026 г.).

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 15.03.2026 г.).

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (последняя редакция) https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 15.03.2026 г.).

4. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст). Электронный ресурс http://bolid.ru/files/552/730/h_2028bcfdb36e8efef0a9a131aee84e45 (дата обращения: 15.03.2026 г.).

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 15.03.2026 г.)

6. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646 https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 15.03.2026 г.).

7. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» https://www.consultant.ru/document/cons_doc_LAW_80028/b14c473967d9079615e7eaa8f79bd5489a1803bd/ (дата обращения: 15.03.2026 г.).

8. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 15.03.2026 г.).

9. Приказ ФСТЭК Российской Федерации от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 15.03.2026 г.).

10. Приказ ФСТЭК Российской Федерации от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» https://normativ.kontur.ru/document?moduleId=1&documentId=500478 (дата обращения: 15.03.2026 г.).

11. Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» https://www.consultant.ru/document/cons_doc_LAW_32924/ (дата обращения: 15.03.2026 г.).

12. Приказ ФСБ Российской Федерации от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» https://www.consultant.ru/document/cons_doc_LAW_167862/3faa8723e46ecc4973f2bc794c221b88debfcaa9/ (дата обращения: 15.03.2026 г.).

Основная литература:

1. Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – М. : РИОР : ИНФРА-М, 2025. – 336 с.

2. Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. – 2-е изд. – Москва : Ай Пи Ар Медиа, 2026. – 130 с. – ISBN 978-5-4497-2349-9. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/155918.html (дата обращения: 15.03.2026 г.). – Режим доступа: для авторизир. пользователей.

3. Основы информационной безопасности. Курс ИНТУИТ, 2016 https://intuit.ru/studies/courses/10/10/info (дата обращения: 15.03.2026 г.).

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2023. – 201 с. – (Высшее образование: Бакалавриат). – DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987 (дата обращения: 15.03.2026 г.). – Режим доступа: по подписке.

5. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 3-е изд. – Саратов : Профобразование, 2024. – 702 с. – ISBN 978-5-4488-0070-2. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/145912.html (дата обращения: 15.03.2026 г.).

Дополнительная литература:

1. Баженов, Р. И. Интеллектуальные информационные технологии в управлении: учебное пособие / Р. И. Баженов. – Москва: Ай Пи Ар Медиа, 2023. – 124 с. – ISBN 978-5-4497-1864-8. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/127570.html (дата обращения: 15.03.2026 г.).

2. Косоруков, А. А. Цифровизация государственного управления: учебное пособие / А. А. Косоруков. – Москва: Ай Пи Ар Медиа, 2023. – 242 с. – ISBN 978-5-4497-1785-6. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www-iprbookshop-ru.ezproxy.ranepa.ru:2443/117051.html (дата обращения: 15.03.2026 г.).

3. Кульназарова, А. В. Цифровые технологии в рекламе и связях с общественностью: учебник / А. В. Кульназарова. – Москва: Ай Пи Ар Медиа, 2023. – 149 с. –ISBN 978-5-4497-2057-– Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/128352.html (дата обращения: 15.03.2026 г.).

4. Курс «Технологии защиты информации в компьютерных сетях»: Национальный Открытый Университет «ИНСТИТУТ»: https://intuit.ru/studies/curriculums/19922/courses/1300/lecture/25504 2015 VANE bv / (дата обращения: 15.03.2026 г.).

5. Мирошников, А.И. Основы информационной безопасности и защита информации: учебное пособие / Мирошников А.И., Сысоев А.С. – Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. – 107 с. – ISBN 978-5-00175-160-1. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/128718.html (дата обращения: 15.03.2026 г.).

6. Морозова, О. А. Информационные технологии в государственном и муниципальном управлении: учебное пособие для вузов / О. А. Морозова, В. В. Лосева, Л. И. Иванова. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2023. – 142 с. – (Высшее образование). Текст: электронный // Образовательная платформа Юрайт [сайт]. с. 2 – URL: https://urait.ru/bcode/516119/p.2 (дата обращения: 15.03.2026 г.).

7. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. – Москва, Вологда : Инфра-Инженерия, 2024. – 144 с. – ISBN 978-5-9729-1610-8. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/143202.html (дата обращения: 15.03.2026 г.).

Интернет-ресурсы:

- https://securelist.ru/ - Аналитика и отчеты о киберугрозах «Лаборатории Касперского»

Справочные системы:

- https://rt-solar.ru/ Солар официальный сайт компании
- http://nlr.ru/ - Российская национальная библиотека
- https://rusneb.ru/ - Национальная электронная библиотека
- https://www.rsl.ru/ - Российская государственная библиотека
- https://www.rambler.ru/ - Поисковая система
- https://yandex.ru/ - Поисковая система
- http://www.consultant.ru/ - Консультант плюс
- https://www.garant.ru/ - Гарант

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Итоговая аттестация проводится в виде зачета в форме тестирования (с применением ДОТ).

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

Оценка качества освоения программы проводится в отношении соответствия результатов освоения программы заявленным целям и планируемым результатам обучения.

Слушатели, успешно прошедшие итоговую аттестацию, получают соответствующий документ о повышении квалификации установленного Академией образца: удостоверение о повышении квалификации.

Слушатели, не прошедшие итоговую аттестацию или получившие на итоговой аттестации неудовлетворительные результаты, вправе пройти повторно итоговую аттестацию в сроки, определяемые образовательной организацией.

Слушателям, не прошедшим итоговую аттестацию по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтвержденных), должна быть предоставлена возможность пройти итоговую аттестацию без отчисления из организации, в соответствии с медицинским заключением или другим документом, предъявленным слушателем, или с восстановлением на дату проведения итоговой аттестации.

Слушателям, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, выдается справка об обучении или о периоде обучения по образцу, самостоятельно установленному образовательной организацией.

Итоговая аттестация слушателей осуществляется без создания итоговой аттестационной комиссии преподавателем(-ями), реализующим(-ими) данную программу.

Примерные вопросы для подготовки к итоговой аттестации

Инструкция для слушателя: выберите один или несколько правильных вариантов ответов

1. Информационный объект – это:

а) аппаратная часть информационной инфраструктуры, хранящая данные;

б) файлы (документы), ресурсы локальных и глобальных сетей;

в) среда, в которой информация создается, передается, обрабатывается или хранится;

г) файлы (документы), сайты, порталы, средства их создания.

2. Является ли информационное общество реализацией экономического и технологического уклада?

а) да;

б) нет.

3. Информационное общество — это общество, в котором:

а) большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей её формы — знаний;

б) постоянно растет количество интернет-пользователей;

в) реализованы технологии электронного управления и электронного правительства;

г) электронная коммерция является преобладающей экономической моделью.

4. Основными компонентами информационного пространства являются:

а) пользователи, информационные ресурсы, провайдеры;

б) владельцы, провайдеры, информационная инфраструктура;

в) информационные ресурсы, средства информационного взаимодействия, информационная инфраструктура;

г) государство, владельцы, посредники.

5. Субъектами информационного пространства являются:

а) государство, юридические лица, физические лица;
б) пользователи, провайдеры, владельцы информации;
в) государство, пользователи, владельцы информации;
г) физические лица, юридические лица, посредники.

6. Принцип расширения субъектности информационного пространства заключается в:
а) увеличении объема передаваемой по Интернет информации;
б) увеличении количества интернет-провайдеров;
в) увеличении количества пользователей глобальной сети во всех странах;
г) это тенденция к вовлечению в современный информационный процесс новых субъектов, в том числе в виде негосударственных образований.

7. По данным Главного информационного центра МВД России, количество компьютерных преступлений ежегодно увеличивается в __ раза (во сколько раз):
а) 2;
б) 2,5;
в) 3,5;
г) 4.

8. По данным Главного информационного центра МВД РФ, средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн. руб.):
а) 0,5;
б) 1,7;
в) 2,5;
г) 3.

9. Компьютерные преступления – это те преступления, в которых:
а) с помощью несанкционированного доступа нарушается конфиденциальность информации;
б) результатом является нарушение системы безопасности предприятия;
в) объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер;
г) нарушается целостность и достоверность информации.

10. Конфиденциальность информации — это:
а) обеспечение доступа к информации тем лицам, у которых есть на это право;
б) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
в) обеспечение защиты той части информации в организации, которая является коммерческой тайной;
г) статус определенной части информации предприятия, который предоставляется для регламентации ее распространения.

Таблица 4.1

Критерии оценки слушателя на итоговую аттестацию

Оценка	Требования к знаниям
зачтено	Выставляется слушателю, если он правильно выполнил более 60% заданий
не зачтено	Выставляется слушателю, если он правильно выполнил менее 60% заданий

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы следующие компетенции:

Таблица 5.1

Характеристика результатов освоения программы

Компетенция (код, содержание)	Индикаторы
ОПК-1[1] Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	- знает базовый понятийный аппарат в области информационной безопасности; - знает виды угроз информационным системам, а также методы обеспечения информационной безопасности; - умеет идентифицировать базовые угрозы для рабочего места и организации; - умеет использовать современные программные и аппаратные средства для защиты информации на рабочем месте
ОПК-5[1] Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	- знает нормативные правовые и организационные основы защиты информации в Российской Федерации; - умеет применять требования 149-ФЗ, 152-ФЗ, 187-ФЗ в повседневной деятельности
ПСК-1[2] Способен организовать обработку и защиту персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ и подзаконных актов	- знает правовой режим персональных данных (ПДн); - знает обязанности оператора; правила деперсонификации и обезличивания; - знает порядок получения и отзыва согласия на обработку ПДн; - знает требования к трансграничной передаче и локализации данных; - знает обеспечение безопасности персональных данных в Российской Федерации; - умеет разрабатывать локальные акты об обработке ПДн; - умеет получать согласие на обработку ПДн; - умеет обеспечивать уничтожение ПДн по требованию субъекта или по истечении срока хранения

ПСК-2[2] Способен применять программно-аппаратные и криптографические средства защиты информации в повседневной деятельности	- знает технологии обеспечения информационной безопасности, способы противодействий киберугрозам и социальным атакам; - знает принципы работы антивирусных средств, межсетевых экранов, систем обнаружения вторжений; - основы применения средств криптографической защиты информации (СКЗИ), включая КриптоПро CSP и VipNet; - правила работы с электронной подписью (ЭП); - умеет настраивать антивирусную защиту; - умеет использовать СКЗИ для шифрования каналов связи и ЭДО; - умеет проверять сертификаты ключей проверки ЭП
ОПК-5[3] Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг	- знает требования нормативных правовых актов в области защиты государственной тайны и конфиденциальной информации при работе в государственных информационных системах (ГИС); - знает основные требования ФСТЭК и ФСБ к защите ГИС; - знает правила работы с конфиденциальными документами; - умеет анализировать крупные массивы данных с использованием современных программных средств; - умеет применять инструменты цифровой культуры в принятии организационно-управленческих решений; - умеет выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - умеет применять полученные знания при выполнении должностных обязанностей
ПСК-3[2] Способен выявлять и противодействовать атакам с использованием методов социальной инженерии (фишинг, вишинг, смишинг), а также участвовать в реагировании на инциденты информационной безопасности	- знает признаки фишинговых писем и подозрительных звонков; - знает способы противодействий киберугрозам и социальным атакам; - знает методы телефонного мошенничества и защиты от спама; - знает правила безопасного использования мессенджеров и социальных сетей; - умеет распознавать фишинговые атаки; - умеет не переходить по подозрительным ссылкам;

	- умеет применять двухфакторную аутентификацию; оперативно блокировать доступ при инцидентах
ПСК-4[2] Способен безопасно работать в системах электронного документооборота (СЭД) и на Едином портале государственных и муниципальных услуг (ЕПГУ), обеспечивая сохранность учетных данных и ключей ЭП	- знает способы информационной безопасности при работе с ЭДО и государственными услугами; - знает типовые схемы мошенничества с аккаунтами Госуслуг; - знает правила подтверждения входа в ЕСИА; - знает сроки действия сертификатов ЭП; - знает порядок действий при утере носителя (Рутокен/флешка) с ключом ЭП или компрометации пароля; - умеет распознавать попытки перехвата учетной записи через фишинговые страницы Госуслуг; - умеет использовать подтвержденную учетную запись только на официальных ресурсах; - умеет своевременно менять пароли доступа к ЕСИА; - умеет оперативно блокировать доступ