Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт «Высшая школа государственного управления»
Центр «Цифровая школа госуправления»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 458F8CD8698157343F17480C0CF8B0A9
Владелец: Кондратенко Олег Игоревич
Действителен: с 19.03.2026 до 12.06.2027

«УТВЕРЖДАЮ»
Директор Института ВШГУ РАНХиГС
О.И. Кондратенко
«08» октября 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ ПРИ ПРИМЕНЕНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ИСПОЛЬЗОВАНИИ ИНТЕРНЕТ-СЕРВИСОВ»

(наименование программы)

Москва, 2026

Разработчик:

И.М. Лапшин,
директор программ центра «Цифровая школа госуправления»
Института ВШГУ РАНХиГС

Руководитель программы:

Ф.Р. Гадзаов,
директор центра «Цифровая школа госуправления»
Института ВШГУ РАНХиГС,
кандидат экономических наук

Дополнительная профессиональная программа повышения квалификации рассмотрена на заседании ученого совета Института ВШГУ, рекомендована к реализации, протокол № 41 от «08» октября 2026 года.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ 4
1.1. Цель и задачи реализации программы 4
1.2. Нормативные правовые акты 4
1.3. Планируемые результаты обучения 6
1.4. Категория слушателей 9
1.5. Формы и технологии обучения 9
1.6. Период обучения, срок освоения и режим занятий 9
1.7. Документ о квалификации 9
2. СОДЕРЖАНИЕ ПРОГРАММЫ 10
2.1. Календарный учебный график 10
2.2. Учебный план 11
2.3. Содержание программы по темам 13
3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ 15
3.1. Материально-техническое и программное обеспечение 15
3.2. Учебно-методическое и информационное обеспечение 15
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ 18
5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ 21

Приложение № 1. Сведения о профессорско-преподавательском составе и ведущих специалистах (кадровая справка)[1]

[1] Кадровая справка не входит в состав программы и формируется отдельно.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации *«Обеспечение информационной безопасности в деятельности органов местного самоуправления при применении цифровых технологий и использовании интернет-сервисов»* разработана в соответствии с перечнем поручений Президента Российской Федерации по итогам заседания Совета при Президенте по развитию местного самоуправления, состоявшегося 20 апреля 2023 г., по вопросам развития кадрового потенциала муниципальной службы и направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности.

1.1. Цель и задачи реализации программы

Целью реализации программы является совершенствование профессиональных компетенций, необходимых для организации безопасной работы с информацией, информационными системами и цифровыми сервисами, защиты персональных данных и обеспечения устойчивости муниципальных функций при возникновении инцидентов информационной безопасности.

Задачи реализации программы:

1. сформировать понимание информационной безопасности как управленческой ответственности, связанной с непрерывностью муниципальных услуг, соблюдением прав граждан, бюджетными и репутационными рисками;
2. научить определять требования законодательства, применимые к муниципальному процессу, информационной системе или цифровому сервису;
3. сформировать навыки выявления информационных активов, основных угроз и уязвимых организационных процессов;
4. отработать правила безопасной работы с персональными данными, электронной почтой, интернет-сервисами, облачными решениями, мессенджерами, мобильными устройствами и общедоступными сервисами искусственного интеллекта;
5. научить распределять роли между руководителем, ответственным за информационную безопасность, ИТ-подразделением, владельцами процессов, кадровой, юридической и закупочной службами, подведомственными организациями и подрядчиками;
6. освоить порядок первичных действий при инциденте, внутренней эскалации, фиксации сведений об инциденте, восстановления работы и разбора причин.

1.2. Нормативные правовые акты

Программа разработана с учетом следующих нормативных правовых актов и методических документов:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. 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».

3. Приказ Минобрнауки России от 12.09.2013 № 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования».

4. Приказ РАНХиГС от 20.04.2026 № 02-00742/001 «Об утверждении порядка реализации дополнительных профессиональных программ в Академии».

5. Приказ РАНХиГС от 02.12.2025 № 02-02669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ – программ повышения квалификации, программ профессиональной переподготовки».

6. Приказ РАНХиГС от 13.01.2026 №02-00010/001 «Об утверждении правил приема на обучение по дополнительным профессиональным программам в Академию».

7. Приказ от 13 января 2026 года № 02-00009/001 «Об утверждении Положения об итоговой аттестации слушателей дополнительных профессиональных программ в Академии».

8. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление, утвержденный приказом Министерства науки и высшего образования РФ от 13 августа 2020 г. № 1016.

9. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

10. Федеральный закон от 20.03.2025 № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти».

11. Федеральный закон от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации».

12. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

13. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

14. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

15. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

16. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

17. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

18. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

19. Распоряжение Правительства Российской Федерации от 22.12.2022 № 4088-р об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации.

20. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

21. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

22. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

23. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (в редакции приказа ФСТЭК России от 08.05.2026 № 137; применяется в пределах установленной сферы действия).

24. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

25. ОК 010-2014 (МСКЗ-08). Общероссийский классификатор занятий» (принят и введен в действие приказом Росстандарта от 12.12.2014 № 2020-ст).

26. Единый справочник должностей руководителей, специалистов и других служащих, установленный постановлением Правительства РФ 31.10.2002 № 787.

27. Справочник типовых квалификационных требований для замещения должностей муниципальной службы (утв. Минтрудом России).

1.3. Планируемые результаты обучения

Таблица 1.3.1

Перечень компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	**Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, ПЛК, ФЗУ)** ***(формируются и (или) совершенствуются)***	**Практический опыт**	**Знания**	**Умения**
ВД 1. Организационно-управленческая	ОПК-5[2] - Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг	*Владеть навыками:* применения современных цифровых технологий, инструментов в автоматизации процессов в муниципальном управлении; владение навыками внедрения знаний по информационной безопасности в сферу профессиональной деятельности	*Знать:* Правовое регулирование защиты информации и персональных данных; виды информации и режимы доступа; ответственность работников, владельцев процессов и подрядчиков; базовые организационные и технические меры; управление доступом, резервное копирование, контроль поставщиков	*Уметь:* Определять применимые требования; выявлять основные риски процесса; формулировать требования безопасности к сервису и подрядчику; распределять ответственность; выбирать приоритетные меры с учетом ресурсов муниципалитета

[2] 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.

Виды деятельности	Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, ПЛК, ФЗУ) *(формируются и (или) совершенствуются)*	Практический опыт	Знания	Умения
ВД 2. Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	ПСК-1[3]. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	*Владеть навыками:* включения в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; уничтожения (стирания) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания); физического уничтожения машинных носителей информации, обрабатываемой автоматизированной системой; архивирования информации, обрабатываемой автоматизированной системой	*Знать:* процедуры архивирования информации, обрабатываемой автоматизированной системой; назначение и принципы работы основных узлов современных технических средств информатизации; организацию технического обслуживания и ремонта компонентов автоматизированной системы; процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации; нормативные правовые акты в области защиты информации; основные методические и руководящие документы уполномоченных	*Уметь:* использовать программные средства для архивирования информации; использовать программные и программно-аппаратные средства для уничтожения (стирания) информации и носителей информации; использовать типовые криптографические средства защиты информации, в том числе электронную подпись

[3] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н (трудовая функция A/03.5)

Виды деятельности	Общепрофессиональные, профессионально-специализированные компетенции или трудовые функции (ОПК, ПСК, ПЛК, ФЗУ) *(формируются и (или) совершенствуются)*	Практический опыт	Знания	Умения
ВД 3. Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	ПСК-2 [4] . Управление защитой информации в автоматизированных системах	*Владеть навыками:* анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность; составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; оценки последствий от реализации угроз безопасности информации в автоматизированной системе; анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	*Знать:* основные методы управления защитой информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам; нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	*Уметь:* оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные ресурсы автоматизированных систем; применять нормативные документы по защите от несанкционированного доступа к информации и противодействию технической разведке; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; конфигурировать параметры системы защиты информации автоматизированных систем; применять технические средства контроля эффективности мер защиты информации

[4] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н (трудовая функция B/03.6)

1.4. Категория слушателей

К освоению программы допускаются муниципальные служащие, представители местного самоуправления и муниципального сообщества, имеющие среднее профессиональное и (или) высшее образование, и иные лица, получающие среднее профессиональное и (или) высшее образование, без специальной технической подготовки в области информационной безопасности.

1.5. Формы и технологии обучения

Форма и технологии обучения: очная (с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ).

1.6. Период обучения, срок освоения и режим занятий

Период обучения по программе: 1 неделя 5 дней.

Срок освоения программы: 40 академических часов, из них 20 академических часов контактной работы со слушателем с применением ДОТ, 20 академических часов с применением ЭО (18 академических часов самостоятельной работы и 2 академических часа итоговой аттестации).

Режим занятий:

– контактная работа с применением ДОТ – 3 дня в неделю по 2-4 академических часа;

– самостоятельная работа с применением ЭО – 2 дня в неделю по 2-4 академических часа.

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

2.1. Календарный учебный график

Таблица 2.1.1

Календарный учебный график

Период обучения – 1 неделя 5 дней											
1 неделя							5 дней				
1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день	9 день	10 день	11 день	12 день
УЗ ДОТ	СР ЭО	УЗ ДОТ	СР ЭО	УЗ ДОТ	ВД	ВД	УЗ ДОТ	СР ЭО	УЗ ДОТ	УЗ ДОТ СР ЭО	ИА ЭО

УЗ ДОТ – учебные занятия с применением дистанционных образовательных технологий.
СР ЭО – самостоятельная работа с применением электронного обучения.
ИА ЭО – итоговая аттестация с применением электронного обучения.
ВД – выходной день.

2.2. Учебный план

Таблица 2.2.1

Учебный план

по дополнительной профессиональной программе повышения квалификации
«Обеспечение информационной безопасности в деятельности органов местного самоуправления при применении цифровых технологий и использовании интернет-сервисов»

№ 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 (ЭО), час	Текущий контроль успеваемости, час.	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.	Информационная безопасность как управленческая задача органа местного самоуправления. Правовые требования и ответственность	**8**	-	-	-	-	-	-	**4**	4	-	-	-	4	-	-	-	ПСК-1 ПСК-2
2.	Актуальные угрозы и безопасная повседневная работа с цифровыми технологиями	**6**	-	-	-	-	-	-	**4**	4	-	-	-	2	-	-	-	ОПК-5 ПСК-1 ПСК-2
3.	Защита персональных данных и информации ограниченного доступа в муниципальных процессах	**8**	-	-	-	-	-	-	**4**	4	-	-	-	4	-	-	-	ОПК-5 ПСК-1 ПСК-2
4.	Организация системы информационной безопасности муниципалитета	**8**	-	-	-	-	-	-	**4**	4	-	-	-	4	-	-	-	ОПК-5 ПСК-1 ПСК-2

5.	Управление инцидентами и обеспечение непрерывности муниципальных функций	**8**	-	-	-	-	-	-	**4**	4	-	-	-	4	-	-	-	ОПК-5 ПСК-1 ПСК-2
	Итого:	**38**							**20**	**20**				**18**				
	Итоговая аттестация:	**2**	**тестирование с применением ЭО**														**2/З[5]**	
	Всего:	**40**							**20**	**20**				**18**			**2**	

[5] Итоговая аттестация проводится в виде зачета в форме проведения электронного тестирования в системе дистанционного обучения.

2.3. Содержание программы по темам

Таблица 2.3.1

Содержание программы по темам

Номер темы и ее наименование	Содержание темы
Тема 1. Информационная безопасность как управленческая задача органа местного самоуправления. Правовые требования и ответственность	Информационные активы органа местного самоуправления. Связь информационной безопасности с доступностью муниципальных услуг, исполнением полномочий, защитой прав граждан, бюджетными и репутационными последствиями. Виды информации и режимы доступа. Нормативное регулирование защиты информации, персональных данных, электронной подписи и открытости деятельности органов местного самоуправления. Определение применимости требований к государственным информационным системам и критической информационной инфраструктуре. Ответственность руководителей, работников и подрядчиков. Локальные нормативные акты.
Тема 2. Актуальные угрозы и безопасная повседневная работа с цифровыми технологиями	Фишинг, социальная инженерия, компрометация учетных записей, вредоносные вложения, программы-вымогатели, подмена платежных реквизитов, атаки на сайты и сервисы, риски подрядчиков. Пароли и многофакторная аутентификация. Безопасная работа с электронной почтой, файлами, съемными носителями, мобильными устройствами и удаленным доступом. Обновления, резервное копирование и разграничение доступа на уровне, необходимом руководителю и пользователю.
Тема 3. Защита персональных данных и информации ограниченного доступа в муниципальных процессах	Жизненный цикл персональных данных: сбор, правовое основание, минимизация, доступ, передача, хранение, архивирование и уничтожение. Обращения граждан, кадровые документы, сайты, электронные формы, фото- и видеоматериалы. Передача данных подрядчикам и подведомственным организациям. Электронная подпись и юридически значимый обмен. Риски публичных облачных сервисов, мессенджеров и общедоступных сервисов искусственного интеллекта. Ограничения на загрузку реальных персональных данных и служебной информации во внешние сервисы.

Номер темы и ее наименование	Содержание темы и учебная деятельность
Тема 4. Организация системы информационной безопасности муниципалитета	Роли руководителя, ответственного за информационную безопасность, ИТ-подразделения, владельцев процессов и данных, кадровой, юридической и закупочной служб. Реестр информационных активов и учетных записей. Предоставление, изменение и прекращение доступа. Резервное копирование и проверка восстановления. Контроль обновлений и изменений. Журналирование событий. Требования к закупкам, договорам, уровню сервиса и действиям поставщика при инциденте. Обучение работников. Показатели состояния информационной безопасности, внутренний контроль и планирование ресурсов.
Тема 5. Управление инцидентами и обеспечение непрерывности муниципальных функций	Признаки и классификация инцидентов. Каналы информирования и порядок внутренней эскалации. Разрешенные первичные действия работника и руководителя. Фиксация и сохранение сведений об инциденте. Взаимодействие с подрядчиком, уполномоченными органами и правоохранительными органами с учетом применимого правового режима. Коммуникация с гражданами и работниками. Восстановление муниципальной функции, разбор причин и корректирующие меры.

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое и программное обеспечение

Информационно-образовательная среда программы включает электронные информационные ресурсы и электронные образовательные ресурсы, совокупность информационных технологий и телекоммуникационных средств, обеспечивающих освоение программы независимо от места нахождения слушателей. В рамках среды обеспечиваются: размещение учебно-методических материалов, доступ к заданиям и материалам, фиксация результатов обучения, проведение итоговой аттестации, а также обмен сообщениями и обратная связь по вопросам содержания обучения.

Технологические платформы и адреса размещения:

- сервис видеоконференцсвязи для проведения вебинаров: «МТС Линк» https://mts-link.ru

- система дистанционного обучения для размещения материалов, организации самостоятельной работы и проведения итоговой аттестации: Система дистанционного обучения Института ВШГУ https://portal.gosedu.ru/

Материально-технические и программные требования к участникам (обеспечиваются слушателями самостоятельно):

- персональный компьютер или ноутбук (рекомендуется) либо иное устройство, обеспечивающее устойчивую работу с веб-сервисами;

- веб-камера и микрофон (рекомендуется использование гарнитуры);

- установленный современный веб-браузер и программные средства просмотра учебных материалов;

- возможность работы с офисными документами и презентациями (например, Microsoft Office: Word, Excel, PowerPoint и др., либо совместимые программные продукты);

- устойчивый доступ к сети Интернет, обеспечивающий участие в видеоконференциях и работу в СДО.

Коммуникация в процессе обучения: в ходе освоения программы слушатели имеют возможность задавать вопросы преподавателям и организаторам в рамках онлайн-занятий и через каналы связи, используемые в образовательной среде. Для оперативного информирования и организационного сопровождения может применяться общедоступный мессенджер Max или Telegram.

Оснащенность рабочего места преподавателя (обеспечивается организацией): при необходимости для проведения вебинаров используется рабочее место преподавателя, оснащённое компьютером или ноутбуком, средствами аудио- и видеосвязи (веб-камера, микрофон/гарнитура), а также доступом к сети Интернет и к платформам «МТС Линк» и СДО ВШГУ.

3.2. Учебно-методическое и информационное обеспечение

Методические материалы по темам программы размещаются в Системе дистанционного обучения Института ВШГУ и используются при проведении

вебинаров и в рамках самостоятельной работы слушателей. По темам электронного курса предусматриваются:

- учебно-методические материалы (презентации, конспекты/тезисы, дополнительные материалы);
- перечень ключевых вопросов и понятий, контрольные вопросы для самопроверки;
- практико-ориентированные задания;
- ссылки на электронные ресурсы, необходимые для освоения темы.

Содержание учебного материала раскрывается в логической последовательности тем учебного плана с учетом современных подходов к цифровой трансформации, развития науки и техники, а также перспектив их развития.

Самостоятельная работа осуществляется с применением ЭО. Слушатели самостоятельно изучают материалы электронного курса «Обеспечение информационной безопасности в деятельности органов местного самоуправления при применении цифровых технологий и использовании интернет-сервисов» и выполняют задания.

Итоговая аттестация проводится в форме электронного тестирования в Системе дистанционного обучения Института ВШГУ. Учебно-методическое обеспечение итоговой аттестации включает:

- программу и регламент проведения итоговой аттестации (время, порядок доступа, правила прохождения);
- перечень проверяемых результатов обучения;
- банк тестовых заданий (закрытые вопросы с выбором одного/нескольких правильных ответов, задания на установление соответствия, задания на установление последовательности);
- критерии оценивания результатов тестирования и порядок фиксации результата;
- техническую инструкцию по прохождению теста и рекомендации по устранению типовых технических затруднений.

Нормативные правовые документы:

1. Федеральный закон от 20.03.2025 № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти».
2. Федеральный закон от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации».
3. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

7. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

8. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

9. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

10. Распоряжение Правительства Российской Федерации от 22.12.2022 № 4088-р об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации.

11. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

12. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

13. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

14. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (в редакции приказа ФСТЭК России от 08.05.2026 № 137; применяется в пределах установленной сферы действия).

Основная литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. Москва: РИОР, 2025. 336 с. ISBN 978-5-369-01761-6.

2. Сычев Ю.Н. Основы информационной безопасности: учебное пособие. Москва: ИНФРА-М, 2026. 337 с. ISBN 978-5-16-018225-4.

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; под ред. Т.А. Поляковой, А.А. Стрельцова. Москва: Юрайт, 2016. 325 с. ISBN 978-5-9916-6799-9.

Официальные информационные ресурсы

1. Официальный интернет-портал правовой информации: https://pravo.gov.ru/

2. ФСТЭК России: https://fstec.ru/

3. Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/

4. ФСБ России: https://www.fsb.ru/
5. Национальный координационный центр по компьютерным инцидентам: https://cert.gov.ru/
6. Роскомнадзор: https://rkn.gov.ru/
7. Портал персональных данных Роскомнадзора: https://pd.rkn.gov.ru/
8. Минцифры России: https://digital.gov.ru/
9. ВШГУ Президентской академии, Центр «Цифровая школа госуправления»: https://gspm.ranepa.ru/departamentyi/direkcziya-metodologii-i-texnologij-obrazovaniya/czentr-czifrovaya-shkola-gosupravleniya/

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Итоговая аттестация проводится в виде зачета в форме проведения электронного тестирования в системе дистанционного обучения Института «Высшая школа государственного управления».

Процедура итоговой аттестации включает:

- прохождение тестирования на образовательном портале по расписанию программы;
- выполнение теста в установленные сроки;
- автоматизированную обработку результатов, фиксацию результата и хранение данных в информационной системе.

Итоговая аттестация является обязательной для слушателей, завершающих обучение по программе. Итоговая аттестация проводится в форме электронного тестирования в системе дистанционного обучения Института ВШГУ.

Оценочные средства включают:

- итоговый тест (электронное тестирование), охватывающий содержание всех тем программы;
- банк тестовых заданий, из которого формируется индивидуальный вариант теста (вопросы могут выбираться из разных тем; варианты ответов могут перемешиваться);
- задания разных типов: вопросы с выбором одного правильного ответа, вопросы с выбором нескольких правильных ответов, задания на установление соответствия и последовательности, ситуационные задачи.

Методы контроля, позволяющие оценить приобретенные знания, умения и практический опыт:

- оценка знаний - через проверку понимания понятий, принципов и нормативно-организационных механизмов цифровой трансформации и кибербезопасности;
- оценка умений - через ситуационные вопросы на выбор управленческого решения (стратегия, портфель, архитектура, коммуникации, изменения);
- оценка практического опыта (в тестовом формате) - через кейсовые задания, где требуется применить управленческие инструменты (например: выбор метрик, приоритизация инициатив, выбор модели взаимодействия со стейкхолдерами, определение мер управления рисками).

Процесс тестирования должен быть автоматизирован, а результаты - фиксироваться и храниться в системе с соблюдением требований к обработке персональных данных.

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

Слушатели, успешно прошедшие итоговую аттестацию, получают соответствующие документы о повышении квалификации, форму которых образовательная организация устанавливает самостоятельно: 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 аттестационной комиссией, созданной образовательной организацией в соответствии с локальными нормативными актами организации из числа сотрудников РАНХиГС и других организаций.

Примеры заданий для итоговой аттестации

Инструкция для слушателя: выберите один правильный вариант ответа. В итоговый вариант включаются также задания, требующие анализа ситуации.

1. Работник получил в мессенджере просьбу срочно направить файл с персональными данными жителей. Какое действие является безопасным?

A. Немедленно отправить файл, если сообщение подписано фамилией руководителя.
B. Проверить личность и полномочия отправителя по утвержденному каналу, затем действовать по установленному порядку передачи данных.
C. Опубликовать файл в общем облачном хранилище и направить ссылку.
D. Отправить файл с личной электронной почты, чтобы ускорить работу.

2. Что означает принцип минимизации персональных данных?

A. Собирать и обрабатывать только те данные, которые необходимы для конкретной законной цели.
B. Хранить все полученные данные без ограничения срока.
C. Передавать данные всем участникам процесса для ускорения работы.
D. Заменять согласие гражданина устным разрешением руководителя.

3. Что должен сделать работник при признаках компрометации своей учетной записи?

A. Самостоятельно удалить журналы событий и подозрительные файлы.
B. Продолжить работу до подтверждения факта атаки.
C. Незамедлительно сообщить по установленному каналу, зафиксировать признаки и выполнять указания ответственных лиц.
D. Опубликовать сведения об инциденте в социальной сети.

4. Можно ли автоматически считать любую муниципальную информационную систему объектом критической информационной инфраструктуры?

A. Да, любая система органа местного самоуправления является объектом КИИ.
B. Нет, применимость требований определяется по субъекту, сфере деятельности и критериям, установленным законодательством.
C. Да, если в системе обрабатываются документы в формате PDF.
D. Нет, муниципальные организации полностью исключены из законодательства об информационной безопасности.

5. Какое правило следует применять при работе с общедоступным сервисом искусственного интеллекта?

A. Загружать полный набор документов, чтобы повысить качество ответа.
B. Использовать только данные и материалы, обработка которых в сервисе разрешена локальными правилами; исключать персональные данные и служебную информацию без надлежащего основания и мер защиты.
C. Передавать сервису логины и пароли для автоматизации работы.
D. Считать любой ответ сервиса официальным решением органа местного самоуправления.

Таблица 4.1

Критерии оценки успеваемости слушателя на итоговой аттестации

Оценка	Требования к знаниям
«зачтено»	Выставляется слушателю, если он выполнил не менее 50 % заданий; глубоко и прочно усвоил программный материал, свободно справляется с вопросами

«не зачтено»	Выставляется слушателю, если он выполнил менее 50%; не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет задания.

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы следующие компетенции.

Таблица 5.1.1

Характеристика результатов освоения программы

Компетенция	Индикаторы
ОПК-5. Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг	— Определяет вид информации и применимые требования; выявляет основные риски муниципального процесса; распределяет роли; формулирует требования к цифровому сервису и подрядчику; составляет обоснованный план первоочередных организационных и технических мер. — Способен организовывать выполнение требований информационной безопасности в муниципальных процессах и при использовании цифровых технологий

Компетенция	Индикаторы
ПСК-1. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	— Владеет навыками включения в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации, уничтожения (стирания) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) физического уничтожения машинных носителей информации, обрабатываемой автоматизированной системой архивирования информации, обрабатываемой автоматизированной системой. — Способен обслуживать системы защиты информации в автоматизированных системах
ПСК-2. Управление защитой информации в автоматизированных системах	— Распознает распространенные признаки угрозы; выбирает безопасный способ обработки и передачи информации; фиксирует признаки инцидента; своевременно уведомляет ответственных лиц; действует по установленному алгоритму; предлагает меры по восстановлению муниципальной функции и предупреждению повторения инцидента. — Способен обеспечивать безопасность информации в автоматизированных системах