ООО «Лаборатория мультимедиа»

«УТВЕРЖДАЮ»
Директор
В.Л. Леонтьев
«19» мая 2026 г.

Федеральное государственное бюджетное образовательное учреждение высшего образования «РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Институт управления
Дирекция «Высшая школа управления»
Центр корпоративного и бизнес-образования

«УТВЕРЖДАЮ»
Директор Института управления
М.В. Хайруллина
«19» мая 2026 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 04087CF40037B31BA54BB5BCAE5381A907
Владелец: Хайруллина Марина Валентиновна
Действителен: с 12.08.2025 до 12.08.2026

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ БИЗНЕСА»

Москва, 2026

Разработчик

Директор дирекции
«Высшая школа управления»
Института управления РАНХиГС  М.В. Леонова

Генеральный директор
ООО «Лаборатория мультимедиа»  В.Л. Леонтьев

Руководитель программы:

Директор программы
«Высшая школа управления»
Института управления РАНХиГС  А.С. Поеров

Руководитель
структурного подразделения:
Директор дирекции
«Высшая школа управления»
Института управления РАНХиГС  М.В. Леонова

Программа повышения квалификации рассмотрена на заседании Ученого совета Института управления и рекомендована к реализации, протокол № 9 от «19» мая 2026г.

Выписка из протокола № 9
заседания Ученого совета Института управления
федерального государственного бюджетного образовательного
учреждения высшего образования
«Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации»

от 19 мая 2026 года

По пункту 6 повестки дня

СЛУШАЛИ: директора центра корпоративного и бизнес-образования дирекции «Высшая школа управления» Института управления Гумилевскую О.В. об утверждении дополнительной профессиональной программы повышения квалификации «Информационная безопасность для бизнеса», реализуемой дирекцией «Высшая школа управления» Института управления.

Указанная программа прошла проверку и согласование специалистами учебно-методического направления Института управления.

ПОСТАНОВИЛИ: по итогам открытого голосования («за» единогласно) утвердить дополнительную профессиональную программу повышения квалификации «Информационная безопасность для бизнеса», реализуемую дирекцией «Высшая школа управления» Института управления.

Председатель Ученого совета
директор Института управления М.В. Хайруллина

И.о. ученого секретаря И.В. Гунина

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Цель и задачи реализации программы

Цель программы: совершенствование и (или) получение слушателями компетенций, необходимых для эффективного использования методов и инструментов обеспечения информационной безопасности в бизнес -среде.

Задачи реализации программы:

- освоить методы выявления и оценки информационных угроз для бизнеса;
- научиться проектировать системы защиты информации с учётом специфики предприятия;
- овладеть практическими навыками применения средств защиты информации;
- понять экономические аспекты информационной безопасности.

Программа повышения квалификации «Информационная безопасность для бизнеса» реализуется в сетевой форме.

Базовой организацией - организацией, осуществляющей образовательную деятельность, в которую обучающийся принят на обучение в соответствии со статьей 55 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» и которая несет ответственность за реализацию сетевой образовательной программы, осуществляет контроль за участием организаций-участников в реализации сетевой образовательной программы является Институт управления РАНХиГС.

ООО «Лаборатория мультимедиа» выступает в качестве организации-участника - организации, осуществляющей образовательную деятельность и реализующей часть сетевой образовательной программы (отдельные учебные предметы, курсы, дисциплины (модули), иные компоненты) и обладающей ресурсами для осуществления образовательной деятельности по сетевой образовательной программе.

1.2. Нормативные правовые акты

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

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Приказ Минобрнауки России от 24.03.2025 N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам"
3. Постановление Правительства РФ от 11 октября 2023 г. № 1678 "Об утверждении Правил применения организациями, осуществляющими

образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ.

4. «Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов» (утв. Минобрнауки России 22.01.2015 № ДЛ-1/05вн).

5. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (Приказ Минтруда России от 14 сентября 2022 г. N 525н код 06.033).

6. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата) (Приказ Министерства науки и высшего образования РФ от 12 августа 2020 г. № 970).

7. Приказ РАНХиГС от 19 апреля 2019 г. № 02-461 «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию» (с изменениями и дополнениями).

8. Приказ РАНХиГС от 02 декабря 2025 года №02-02669/001 «Об утверждении порядка разработки и утверждения в РАНХиГС дополнительных профессиональных программ - программ повышения квалификации, программ профессиональной переподготовки».

9. Приказ РАНХиГС «Об утверждении Правил приема на обучение по дополнительным профессиональным программам в Академию» №02-00010/001 от 13 января 2026 года.

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

11. Приказ РАНХиГС от 22 сентября 2017 года №01-6230 «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

12. Приказ РАНХиГС от 20 апреля 2026 года №02-00742/001 «Об утверждении порядка реализации дополнительных профессиональных программам в Академии»

1.3. Планируемые результаты обучения

Выпускник по программе повышения квалификации «Цифровые навыки для бизнеса», в соответствии с задачами профессиональной деятельности и целями программы должен обладать следующими основными компетенциями:

Таблица 1

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

Виды деятельности	Общепрофессиональные/профессиональные компетенции (ОПК,	Практический опыт	Знания	Умения

	ПК) или трудовые функции (ПСК и СК)			
1	2	3	4	5
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[1]. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	- информирование персонала об угрозах безопасности информации - информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации - ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем	- нормативных правовых актов в области защиты информации - эксплуатационную и проектную документацию на автоматизированную систему -основных методов организации и проведения технического обслуживания технических средств информатизации	- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации - оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации
УК - универсальные компетенции *(формируются и (или) совершенствуются)*				
Универсальные компетенции (УК)	УК-1[2]. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач в области организации производства	— владение методами поиска, сбора и обработки, критического анализа и синтеза информации о состоянии производственной системы. — владение методикой системного подхода для решения задач по повышению эффективности процессов.	— методики поиска, сбора и обработки информации и технологиях. — актуальных российских и зарубежных источников информации — метода системного анализа и выявления коренных причин проблем	анализировать производственную задачу, выделять её базовые составляющие, осуществлять декомпозицию задачи. — находить и критически анализировать информацию, необходимую для решения поставленной задачи по улучшению процесса.

1.4. Категория слушателей

Требования к слушателям программы: наличие высшего или среднего профессионального образования, подтвержденное документами государственного образца.

[1] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (Приказ Минтруда России от 14 сентября 2022 г. N 525н код 06.033), обобщенная трудовая функция А, трудовая функция А/02.5

[2] Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата)

1.5. Формы и технологии обучения

Программа реализуется с использованием сетевой формы. Форма обучения – очно-заочная, с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ).

1.6. Период обучения, срок освоения и режим занятий

Период обучения – 1 неделя.

Общая трудоемкость программы 18 академических часов: часов контактной работы со слушателем – 12, часов самостоятельной работы - 4, часов итоговой аттестации – 2.

Режим занятий: с понедельника по субботу с 09.00 до 16.00.

1.7. Документ о квалификации

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

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Календарный учебный график

Таблица 2

Календарный учебный график

1 нед.
УЗ ЭО и ДОТ , СР, ИА ДОТ

Календарный учебный график содержит следующие условные обозначения:

УЗ ЭО и ДОТ – учебные занятия с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ);

СР – самостоятельная работа;

ИА ДОТ – итоговая аттестация с применением дистанционных образовательных технологий;

2.2 Учебный план

Таблица 3

Учебный план

№п/п	Наименование раздела, модуля, дисциплины, темы, практики, стажировки	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	Промежуточная аттестация (форма/час)	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции/ в интерактивной форме	Практические (семинарские/лабораторные) 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	16	17	18	19	20
Модули, реализуемые Организацией-участником																		
1	Модуль 1 Обеспечение информационной безопасности бизнеса	12						4	8	4	4							ПСК-1,УК-1
Модули, реализуемые Базовой организацией																		
1	Модуль 1 Обеспечение информационной безопасности бизнеса	4							4		4							ПСК-1,УК-1
	Итого:	16						4	12	4	8							
Модули, реализуемые Базовой организацией																		
	Итоговая аттестация	2															З (Д)	
	Всего:	**18**						**4**	**12**	**4**	**8**						**2**	

2.3 Содержание программы по темам

Таблица 4

Содержание программы по темам

Номер темы и ее наименование	Содержание темы
Модуль 1 Обеспечение информационной безопасности бизнеса	– Основы информационной безопасности – Антифишинг – Защита персональных данных – Цифровая гигиена

3.ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое и программное обеспечение реализации программы

РАНХиГС располагает материально-технической базой, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работы, итоговой аттестации слушателей, предусмотренных учебным планом вуза и соответствующей действующим санитарным и противопожарным правилам и нормам.

Минимально необходимый для реализации программы перечень материально-технического обеспечения включает в себя:

✓ лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в Интернет);

✓ помещения для проведения семинарских и практических занятий (оборудованные учебной мебелью);

✓ компьютерные классы с персональными компьютерам.

Программное обеспечение: лицензионные системные программы операционные системы (Windows, 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; использование Интернет, электронной почты; использование автоматизированных поисковых систем Интернет.

Структура информационно-образовательной среды включает:

- образовательный w-портал (сайт) Академии;
- базы данных электронных информационных ресурсов;
- корпоративную сеть Академии.

W- портал (сайт) обеспечивает через Интернет:

- доступ к электронным информационным и образовательным ресурсам Академии;
- доступ к нормативным и организационно-методическим документам, регламентирующим образовательный процесс в Академии;
- систему электронной почтовой пересылки письменных работ слушателей;
- взаимодействие слушателей с преподавателями, организаторами образовательного процесса и администрацией Академии.

Организация учебного процесса по программе основана на технологиях, позволяющих повысить эффективность получаемого образования.

Слушатели программы получают доступ к информационным ресурсам (источникам) и средствам информатизации.

3.2. Учебно-методическое и информационное обеспечение программы

Примеры вопросы для самостоятельных работ:

1. Какие вы знаете источники дестабилизирующего воздействия на информацию?
2. Определите результаты дестабилизирующего воздействия на информацию в зависимости от его вида и способа.
3. Выявление каналов доступа к информации.
4. Методы получения несанкционированного доступа к информации
5. Канал доступа к информации и его связь с и источником воздействия на информацию.
6. ИКТ и вычислительное оборудование как инструментарий автоматизации и информатизации прикладных задач ИБ.
7. Методы оценки качества, надежности и информационной безопасности ИС.
8. Какие задачи решаются с помощью криптографических методов?
9. Законодательная база защиты информации.
10. Защита информации при работе с посетителями.
11. Политика ИБ предприятия и ее структура
12. Политика ИБ: уровни и процедуры.
13. Что включает базовая политика ИБ?
14. Анализ рисков. Риск-ориентированный подход к обеспечению ИБ.
15. Проблема персонала в задачах обеспечения информационной безопасности бизнеса.

Пример задания для практических занятий:

Вопросы:

1. Что именно необходимо отнести к «коммерческой тайне» для Вашего предприятия? Приведите несколько примеров.
2. Составьте перечень угроз информационной безопасности (не менее 5) для рекламного агентства.
3. Назовите объекты, которые необходимо защищать от угроз информационной безопасности для финансового учреждения.
4. Система управления обеспечением ИБ (СУОИБ). Результат реализации меры «описание объекта»?

Описание инфраструктуры объекта

Описание процессов объекта и связи их с процессами организации

Описание активов объекта

5. В процессную модель организации включают:

Основные (бизнес) процессы

Вспомогательные процессы (по видам обеспечения)

Вспомогательные процессы (автоматизация отдельных процессов организации)

Процессы аудита деятельности организации

Процессы мониторинга деятельности организации

6. Система управления обеспечением ИБ (СУОИБ). Этапы идентификации активов объекта:

Определить перечень активов объекта

Определить перечень активов объекта в контексте бизнес-процессов организации

Определить уязвимости активов

7. К активам объекта можно отнести:

Информационные активы

ИТ-сервисы

Нематериальные активы

Объект в целом как часть организации

Организацию в целом

8. Цель реализации меры обеспечения ИБ «Анализ угроз ИБ»?

Сформировать перечень актуальных угроз ИБ

Описать угрозы ИБ

9. Какие меры могут быть использованы при анализе угроз ИБ?

Оценка риска ИБ

Оценивание риска ИБ

Обработка риска ИБ

10.Какой базовый подход используется при анализе угроз ИБ объекта?

Экспертный подход

Процессный подход

11.Какая угроза ИБ признается актуальной?

Уровень риска ИБ, относящийся к этой угрозе, будет превышать риск-аппетит

Уровень риска ИБ, относящийся к этой угрозе, будет равен риск-аппетиту

Уровень риска ИБ, относящийся к этой угрозе, будет меньше риск-аппетита

12.Какими категориями оперирует вербальная методика оценки риска?

степень возможной реализации угрозы ИБ

степень тяжести последствий от угрозы ИБ

вероятность реализации угрозы ИБ

ущерб от реализации угрозы ИБ

13.Может ли сотрудник организации быть внутренним нарушителем?

НЕТ (всегда)

ДА, если он имеет санкционированный доступ к активу, на который направлена конкретная угроза ИБ

ДА (всегда)

НЕТ, если он не имеет санкционированный доступ к активу, на который направлена конкретная угроза ИБ

14.Обработка рисков связана с:

выбором процессов защиты информации

выбором мер защиты информации, реализующие процессы защиты информации

выбором методов защиты информации

15.Что должен содержать реестр рисков в отношении к конкретной угрозе?

величину начального риска ИБ

величину остаточного риска ИБ

величину принятого риска

Нормативно-правовые документы:

Национальные стандарты РФ в области бережливого производства:

1. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 29.12.2025, с изм. от 06.02.2026)

Основная литература:

1.Горбенко, А. О., Безопасность электронного бизнеса : учебное пособие / А. О. Горбенко, А. В. Горбенко. — Москва : КноРус, 2024. — 225 с. — ISBN 978-5-406-11953-2. — URL: https://book.ru/book/950426 — Текст : электронный.

2.Николаев Н.С., Управление информационной безопасностью [Электронный ресурс] : учебник / Н.С. Николаев. - М. : КноРус, 2021. - 188 с. - ISBN 978-5-406-07325-4. - Режим доступа: https://book.ru/book/939841

Дополнительная литература:

3.Мельников В.П., Информационная безопасность [Электронный ресурс] : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. - М. : КноРус, 2023. - 371 с. - ISBN 978-5-406-11960-0. - Режим доступа: https://book.ru/book/950148

4.Бабаш А.В., Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс] : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М. : КноРус, 2023. - 131 с. - ISBN 978-5-406-11731-6. - Режим доступа: https://book.ru/book/949452

Интернет-ресурсы:

5.ЭБС «Znanium». Коллекция учебников по устойчивому развитию и Lean-менеджменту [Электронный ресурс]. — Режим доступа: https://znanium.ru (по подписке РАНХиГС).

6.Образовательная платформа «Юрайт — Режим доступа: https://urait.ru (по подписке РАНХиГС).

7.Цифровая экономика https://xn-- 80aapampemcchfmo7a3c9ehj.xn--p1ai/mediaProjects/mery-podderzhkidlya-roditeley/?utm_source=ano_nationalproject&utm_ medium=cpc&utm_campaign=universal_promo_familysupport&utm_content=b anner_main

8.Журнал "Цифровая экономика" http://digital-economy.ru

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Итоговая форма контроля по программе:

Итоговая аттестация проводится в форме зачета и включает:

• Тестирование

Пример вопросов для итогового тестирования:

1.Естественные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

2. Искусственные угрозы безопасности информации вызваны:

деятельностью человека ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

корыстными устремлениями злоумышленников ошибками при действиях персонала

3. К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

4. К основным преднамеренным искусственным угрозам АСОИ относится:

игнорирование организационных ограничений (установленных правил) при работе в системе

пересылка данных по ошибочному адресу абонента неправомерное отключение оборудования или изменение режимов работы устройств и программ хищение носителей информации

5.Что используется для создания цифровой подписи?

Закрытый ключ получателя

Открытый ключ отправителя

Закрытый ключ отправителя

Открытый ключ получателя

6. Шифрование информации это:

процесс сбора, накопления, обработки, хранения, распределения и поиска информации

преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

7.Атака, которая использует недостатки алгоритмов удаленного поиска (DNS (Internet)…):

подмена доверенного объекта или субъекта распределенной вычислительной сети

ложный объект распределенной вычислительной сети

анализ сетевого трафика

отказ в обслуживании;

удаленный контроль над станцией в сети.

Критерии оценки:

Зачет выставляется при наборе 70 и более баллов из 100 возможных.

5.ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы компетенции:

Таблица 5

Компетенция (код, содержание)	Индикаторы
ПСК-1 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	Знать: современные подходы и стандарты автоматизации организации; технологию документирования процессов создания информационных систем на стадиях жизненного цикла программного обеспечения Уметь: применять международные (ISO), государственные (ГОСТ)и производственные стандарты при разработке автоматизированных информационных систем; планирования работ по определению первоначальных требований заказчика к ИС и возможности их реализации в ИС
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных профессиональных задач в области организации производства	Знания: - технологии саморазвития и профессионального роста работников Умения: - использовать современные технологии развития участников команды Навыки/трудовые действия: - самооценки, самореализации, а также мотивации членов команды для саморазвития

Приложение 2.

С В Е Д Е Н И Я
о преподавательском составе и ведущих специалистах (кадровая справка)

Реализация программы обеспечивается преподавательским составом РАНХиГС, а также высококвалифицированными специалистами из числа руководителей и ведущих специалистов государственных органов, учреждений и иных организаций (включая индивидуальных предпринимателей и самозанятых граждан), в том числе иностранных (далее – ведущие специалисты), а также преподавателями ведущих российских и иностранных образовательных организаций.

Ф.И.О. преподавателя/ведущего специалиста	**Квалификация по диплому о высшем или среднем профессиональном образовании**	**Дополнительн/ая/ые квалификаци/я/и**	**Ученая степень, ученое (почетное) звание**	Стаж работы в области профессиональной деятельности / по дополнительной квалификации	Наименование преподаваемой дисциплины / темы (модуля), практики / стажировки (при наличии) в данной программе
1	2	3	5	6	9
Лебедева Наталья Николаевна	Психолог, Преподаватель психологии по специальности «Психология» (ФГБОУ ВПО «Ярославский государственный университет им. П.Г. Демидова», 2008) Менеджер по специальности «Менеджмент организации» (ФГБОУ ВПО «Ярославский государственный университет им. П.Г. Демидова», 2011)	«Методика преподавания в высшей школе на основе компетентностного подхода» (ФГБОУ ВПО «Ярославский государственный университет им. П.Г. Демидова», 2018) «Профстандарты на предприятии» (ЧУ ДПО «Институт бизнеса «ИПГ «Спектр», 2021)		17 / 7 лет	Обеспечение информационной безопасности бизнеса
Поеров Алексей Сергеевич	Экономист, Московская Академия предпринимательства при Правительстве г. Москвы 2006г.	ДПП ПК «Использование СДО в образовательном процессе с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ)»	Доцент	19 лет	Обеспечение информационной безопасности бизнеса

ВНУТРЕННЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации

«Информационная безопасность для бизнеса»,

разработанную Дирекцией «Высшая школа управления»
Института управления
Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации

В эпоху цифровой трансформации бизнеса и роста числа киберугроз вопросы защиты информации выходят на первый план. Утечки данных, фишинговые атаки и несанкционированный доступ к коммерческой тайне наносят компаниям многомиллионные убытки и подрывают доверие клиентов. При этом многие руководители и сотрудники, не являясь профильными ИТ-специалистами, испытывают дефицит базовых знаний в области информационной безопасности. Рецензируемая программа повышения квалификации «Информационная безопасность для бизнеса» направлена на восполнение этого пробела, формируя у слушателей практические навыки выявления угроз, проектирования систем защиты и экономической оценки мер информационной безопасности.

Программа содержит все необходимые структурные компоненты: общую характеристику, нормативно-правовое обоснование, планируемые результаты обучения, календарный учебный график, учебный план, содержание тем, организационно-педагогические условия, оценочные материалы и индикаторы сформированных компетенций. Разработка соответствует требованиям Федерального закона № 273-ФЗ, приказа Минобрнауки России № 266, профессионального стандарта «Специалист по защите информации в автоматизированных системах» (код 06.033) и ФГОС ВО по направлению подготовки 38.03.02 Менеджмент.

Цель программы — совершенствование компетенций в области использования методов и инструментов обеспечения информационной безопасности в бизнес-среде — достигается через решение комплекса задач: освоение методов выявления и оценки информационных угроз для бизнеса, проектирование систем защиты информации с учётом специфики предприятия, овладение практическими навыками применения средств защиты информации, а также понимание экономических аспектов информационной безопасности.

В процессе обучения у слушателей формируются следующие профессионально-специализированные и универсальные компетенции. **ПСК-1** (ведение технической документации, связанной с эксплуатацией систем

защиты информации автоматизированных систем) предполагает знание нормативных правовых актов в области защиты информации, эксплуатационной и проектной документации на автоматизированную систему, а также основных методов организации и проведения технического обслуживания технических средств информатизации; умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации, а также оформлять техническую документацию в соответствии с нормативными правовыми актами; владение навыками информирования персонала об угрозах и правилах эксплуатации систем защиты информации, а также ведения протоколов и журналов учёта при изменении конфигурации систем защиты информации. **УК-1** (способность к поиску, критическому анализу и синтезу информации) включает знание методик обработки информации и методов системного анализа, умение осуществлять декомпозицию задач и находить необходимую информацию, а также владение методами поиска, сбора и обработки информации о состоянии производственной системы. Данный набор компетенций в полной мере соответствует требованиям профессионального стандарта и реальным запросам работодателей.

Содержательное наполнение программы отличается практической направленностью и лаконичностью. Единственный модуль «Обеспечение информационной безопасности бизнеса» охватывает четыре ключевые темы: «Основы информационной безопасности», «Антифишинг», «Защита персональных данных» и «Цифровая гигиена». Такое построение позволяет слушателям получить системное представление о природе киберугроз, научиться распознавать фишинговые атаки, освоить правила работы с персональными данными клиентов и сотрудников, а также выработать привычки безопасного поведения в цифровой среде — от использования паролей до работы с корпоративной почтой и облачными сервисами.

Практическая ориентированность программы подтверждается характером заданий. Вопросы для самостоятельной работы охватывают широкий спектр тем: от выявления источников дестабилизирующего воздействия на информацию и каналов доступа до законодательной базы защиты информации, политики информационной безопасности предприятия и риск-ориентированного подхода.

Трудоёмкость программы составляет 18 академических часов, из которых 12 часов отведено на контактную работу, 4 — на самостоятельную подготовку и 2 — на итоговую аттестацию. Формат очно-заочного обучения с применением электронных и дистанционных технологий, а также

использование онлайн-курсов с тьюторским сопровождением обеспечивают гибкость и индивидуальный темп освоения материала.

Итоговая аттестация проводится в форме зачета и тестирования. Представленные в программе примеры тестовых вопросов (от классификации естественных и искусственных угроз до механизмов цифровой подписи и типов кибератак) демонстрируют охват всех ключевых тем и адекватность оценочных материалов заявленным результатам обучения.

Таким образом, рецензируемая программа повышения квалификации «Информационная безопасность для бизнеса» представляет собой целостный, логически выстроенный и практико-ориентированный образовательный продукт. Она соответствует нормативным требованиям, профессиональным стандартам и насущным потребностям бизнеса в формировании культуры информационной безопасности. Программа может быть рекомендована к утверждению и реализации для руководителей всех уровней, сотрудников отделов информационной безопасности, менеджеров по работе с данными, а также для всех специалистов, чья деятельность связана с обработкой конфиденциальной информации.

Рецензент:

Коробейникова С.В.
К.э.н., DBA, доцент,
профессор кафедры менеджмента
факультета менеджмента
Института управления РАНХиГС

ВНЕШНЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации

«Информационная безопасность для бизнеса»,

разработанную Дирекцией «Высшая школа управления»
Института управления
Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации

В условиях стремительного роста числа кибератак и ужесточения законодательства в области защиты персональных данных информационная безопасность перестала быть исключительной прерогативой IT-отделов, превратившись в стратегический приоритет для компаний любого масштаба. Представленная на рецензию дополнительная профессиональная программа повышения квалификации «Информационная безопасность для бизнеса» призвана сформировать у слушателей практические компетенции, необходимые для выявления, оценки и нейтрализации информационных угроз в корпоративной среде.

Разработанная Дирекцией «Высшей школы управления» программа ориентирована на формирование у слушателей системного понимания основ информационной безопасности — от классификации угроз и каналов утечки данных до проектирования систем защиты и оценки экономической эффективности мер информационной безопасности. Цель программы — совершенствование компетенций в области использования методов и инструментов обеспечения информационной безопасности в бизнес-среде — достигается через освоение методов выявления и оценки угроз, навыков проектирования систем защиты с учётом специфики предприятия, а также понимание экономических аспектов информационной безопасности.

Ключевые результаты освоения программы напрямую вытекают из содержания четырёх тематических блоков. «Основы информационной безопасности» закладывают понятийный аппарат и знание природы киберугроз. «Антифишинг» формирует навыки распознавания мошеннических рассылок и социальной инженерии — самого распространённого сегодня канала атак. «Защита персональных данных» даёт практические инструменты для соблюдения законодательных требований и защиты данных клиентов и сотрудников. «Цифровая гигиена» завершает логику программы, вырабатывая привычки безопасной работы с паролями, корпоративной почтой, облачными сервисами и съёмными носителями.

Особую ценность программы представляет её нацеленность на выработку конкретных поведенческих алгоритмов, которые слушатели могут немедленно внедрить в свою повседневную практику. Обучение строится не вокруг абстрактных теоретических конструкций, а вокруг реальных сценариев — от анализа рисков для конкретного предприятия до составления перечня угроз для различных отраслей (рекламное агентство, финансовое учреждение). Программа формирует у слушателей навыки идентификации активов, оценки уязвимостей и документального оформления процедур ИБ — то есть всего того, что составляет повседневную работу ответственного сотрудника в области защиты информации.

Программа реализуется в сетевой форме с участием ООО «Лаборатория мультимедиа», что обеспечивает доступ к современным образовательным технологиям и актуальным бизнес-кейсам. Обучение с применением электронных и дистанционных технологий делает программу максимально удобной для занятых профессионалов — руководителей, менеджеров, сотрудников

отделов безопасности и всех, кто работает с конфиденциальной информацией. Учебно-методическое обеспечение включает актуальные издания по безопасности электронного бизнеса и управлению информационной безопасностью, а также доступ к электронно-библиотечным системам.

Рецензируемая программа повышения квалификации «Информационная безопасность для бизнеса» отвечает современным требованиям, предъявляемым к программам данного уровня, и может быть рекомендована для обучения руководителей компаний, менеджеров по персоналу, сотрудников, ответственных за работу с персональными данными, а также всех специалистов, желающих повысить уровень своей цифровой грамотности и защитить бизнес от актуальных киберугроз.

Рецензент:

Каргина Лариса Андреевна, д.э.н., профессор кафедры «Экономической информатики», Федеральное государственное бюджетное учреждение высшего образования «Московский государственный университет путей сообщения Императора Николая II»

/Каргина Л.А.