



Негосударственное образовательное частное учреждение организации дополнительного профессионального образования «Актин»



ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

дополнительного профессионального образования (повышение квалификации)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГОССЕКТОРЕ:

УПРАВЛЕНИЕ РИСКАМИ И ЗАЩИТА ДАННЫХ»

(объем 40 академических часа(ов))

г. Москва

1. ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Программа направлена на освоение (совершенствование) следующих профессиональных компетенций:

- формирование защищенной системы хранения информации;
- поддержание организационно-распорядительной документации по информационной безопасности в актуальном состоянии;
- выявление и отражение информационных атак;
- использование различных способов и инструментов для защиты информации;
- распознавание технологий искусственного интеллекта для предупреждения мошеннических схем;
- владение программно-аппаратными средствами защиты информации.

В результате освоения программы слушатель будет:

знать:

- законодательство Российской Федерации в области информационной безопасности;
- базовые определения и направления защиты информации;
- типы информационных систем и мероприятия по защите информации, которую содержат системы;
- общие мероприятия по защите информации;
- внутренние организационно-распорядительные документы по информационной безопасности;
- модели информационных атак и схемы мошенничества;
- технологии искусственного интеллекта для мошеннических схем;

уметь:

- разрабатывать и сопоставлять с законодательством внутренние документы учреждения об информационной безопасности;
- соблюдать технические требования, предъявляемые к АРМ, подключаемым к информационным системам;
- создавать сложные пароли для разных информационных сервисов;
- использовать двухфакторную авторизацию;
- распознавать мошеннические схемы, созданные искусственным интеллектом;
- использовать защитные инструменты при работе в информационных системах;
- выполнять требования оператора ИС при обмене информацией;
- применять требования закона о персональных данных;
- соблюдать отраслевые требования к защите данных.

2. **НОРМАТИВНЫЕ ДОКУМЕНТЫ** – профессиональный стандарт 08.002 Бухгалтер.
3. **ТРУДОЕМКОСТЬ И СРОК ОСВОЕНИЯ ПРОГРАММЫ** - 40 академических часа(ов), 1 месяц(ев).
4. **ФОРМА ОБУЧЕНИЯ** - заочная с использованием дистанционных образовательных технологий.
5. **УЧЕБНЫЙ ПЛАН**

№ п/п	Наименование дисциплин / модулей (в том числе практик)	Часы			Формы контроля
		Всего часов	Аудиторные	Самостоятельное изучение	
1	2	3	4	5	6
1.	Практика применения требований законодательства об информационной безопасности	39	13	26	-
A	Итоговая аттестация	1	-	1	зачет
	ИТОГО:	40	13	27	-

6. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН ПРОГРАММЫ

№ п/п	Наименование разделов программы	Часы				Содержание разделов программы
		Всего часов	Аудиторные		Самостоятельное изучение	
			Лекции	Практические занятия		
1	2	3	4	5	6	7
1.1.	Структура информационной безопасности	5	1	-	4	Система в информационной безопасности. Базовые определения информационной безопасности. Направления информационной безопасности. Нормативно правовая база по информационной безопасности.
1.2.	Организация информационной безопасности в учреждении	19	8	-	11	Направления информационных атак на российские организации. Негативные последствия атак для организаций.

						Типы информационных систем и мероприятия по защите информации. Виды программно-аппаратных средств защиты информации. Организационно-распорядительные документы по информационной безопасности. Нарушения со стороны работников и противодействие им.
1.3.	Инструменты и способы защиты работников от информационных атак и мошенничества	10	3	-	7	Каналы социальной инженерии против работников. Схемы мошенничества. Способы защиты данных.
1.4.	Противостояние искусственному интеллекту в мошеннических схемах	5	1	-	4	Схемы использования ИИ в социальной инженерии. Способы распознавания ИИ в мошеннических схемах и действия по предотвращению утечки информации.
	ИТОГО:	39	13	-	26	-

7. ЗАДАНИЯ ДЛЯ САМОКОНТРОЛЯ

В процессе обучения с целью проверки качества освоения материала и закрепления пройденных тем слушателю предлагается задание для самоконтроля - тестирование из общего числа вопросов, относящихся к материалам пройденного раздела. Доступ к материалам следующего раздела слушатель получает после того, как ответит не менее, чем на 7 вопросов задания для самоконтроля.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

8.1. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА:

- Белов Е.Б. Основы информационной безопасности: Учебн. пособие
- Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В. - М.: Горячая линия - Телеком, 2005. - 416 с.
- Ушаков Д.В. - М.: Горячая линия - Телеком, 2006. - 686 с.
- Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003. - 192 с.
- Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.-304 с.
- Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006.
- Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2006.
- Язов Ю.К. Основы технологий проектирования систем защиты информации в информационно-телекоммуникационных системах: Монография /Аграновский А.В., Мамай В.И., Назаров И.Г., Язов Ю.К. -Издательство СКНЦ ВШ, 2006.

9. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное - Издательство им."Е.А.Болховитинова, Воронеж, 2011.
10. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - С.-П., 2004.- 384 с.
11. Петраков А.В. Основы практической защиты информации. Учебное пособие. -М., 2005.- 281 с.
12. Девянин П.Н. Садердинов А.А., Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. - М., 2006.- 335.

8.2. НОРМАТИВНО-ПРАВОВЫЕ АКТЫ:

1. Указ Президента РФ от 31.03.2023 № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации "ГосТех"»;
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
4. 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»;
5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
7. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8.3. ДРУГИЕ ИСТОЧНИКИ:

1. Бухгалтерская справочная система «Система Госфинансы» <https://www.gosfinansy.ru/>;
2. Электронный журнал «Учет в учреждении» <https://e.budgetnik.ru/>

9. ИТОГОВАЯ АТТЕСТАЦИЯ

Оценка качества освоения программы осуществляется по результатам прохождения итоговой аттестации. Итоговая аттестация проводится в форме тестирования. Тестирование проводится на платформе дистанционного обучения, результат подсчитывается автоматически. Тест состоит из вопросов, случайным образом выбираемых системой дистанционного обучения из общего числа утвержденных вопросов, так чтобы в тесте были представлены вопросы по всем темам. Ответ не зачитывается при выборе неверного варианта ответа, а также при одновременном указании правильного и неправильного вариантов.

Аттестованным считается слушатель, получивший по результатам прохождения аттестации оценку не ниже «зачтено»:

- оценка «зачтено» выставляется слушателю, верно ответившему не менее чем, на 17 вопросов;
- оценка «не зачтено» выставляется слушателю, верно ответившему на 16 и менее вопросов.

Слушателям, освоившим образовательную программу и успешно прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации (установленного образца).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ ПРОГРАММЫ – программа реализуется с применением дистанционных образовательных технологий и электронного обучения.

11. СОСТАВИТЕЛИ:

1. Галяев В. С., заместитель директора Центра информационно-телекоммуникационных технологий и защиты информации ФГАНУ «ФИЦТО»
2. Казанцева Ю. Е., замдиректора по финансово-экономической работе ГБУ «Мой семейный центр "Молодая гвардия"» Департамента труда и соцзащиты населения города Москвы, преподаватель Школы Главбуха госучреждения.