ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«САПФИР-ЭКСПЕРТ»

САПФИР
ЭКСПЕРТ

УТВЕРЖДАЮ:
Генеральный директор

П.Ю. Ведерников
«01» июня 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ»

Составитель (автор) программы: Крупин Илья Викторович

г. Екатеринбург
2026

1. Общая характеристика программы

1.1. Программа направлена на формирование компетенций в области информационной безопасности, управления рисками, защиты информационных систем и реагирования на инциденты.

1.2. Лицензия № 18710 от 23.05.2016 года на осуществление образовательной деятельности, выданная Министерством общего и профессионального образования Свердловской области. Вид: дополнительное образование. Подвид: Дополнительное профессиональное образование

1.3. Категория слушателей: руководители подразделений, специалисты ИТ-служб, специалисты по информационной безопасности, сотрудники государственных и коммерческих организаций

1.4. Форма обучения:

- очная, очно-заочная, дистанционная
- индивидуально, коллективно (в группе)

1.5. Итоговая аттестация: защита итогового проекта

1.6. Продолжительность обучения: 72 академических часа

2. Цель программы

2.1. Формирование у слушателей практических навыков организации системы информационной безопасности организации

2.2. Формирование у слушателей практических навыков оценки рисков и применения современных средств защиты информации

3. Планируемые результаты обучения

3.1. Слушатель должен знать:

- основы информационной безопасности
- нормативно-правовую базу РФ
- методы оценки рисков
- современные средства защиты информации

3.2. Слушатель должен уметь:

- выявлять угрозы и уязвимости
- проводить оценку рисков
- разрабатывать организационные и технические меры защиты
- анализировать инциденты безопасности

3.3. Слушатель должен владеть:

- методиками управления рисками

• навыками разработки политики ИБ
• инструментами мониторинга безопасности

4. Учебный план

Раздел 1 - Основы информационной безопасности — 8 часов
Раздел 2 - Нормативно-правовое регулирование — 10 часов
Раздел 3 - Управление рисками ИБ — 10 часов
Раздел 4 - Техническая защита информации — 14 часов
Раздел 5 - Безопасность информационных систем — 10 часов
Раздел 6 - Управление инцидентами — 8 часов
Раздел 7 - Социальная инженерия — 6 часов
Раздел 8 - Итоговый проект — 6 часов

5. Содержание программы

Раздел 1. Основы информационной безопасности
Тема 1.1. Информация как объект защиты
Тема 1.2. Конфиденциальность, целостность, доступность
Тема 1.3. Актуальные угрозы кибербезопасности

Раздел 2. Нормативно-правовое обеспечение
Тема 2.1. Законодательство РФ
Тема 2.2. Персональные данные
Тема 2.3. Требования ФСТЭК и ФСБ России

Раздел 3. Управление рисками
Тема 3.1. Активы организации
Тема 3.2. Анализ угроз и уязвимостей
Тема 3.3. Формирование реестра рисков

Раздел 4. Техническая защита информации
Тема 4.1. Защита рабочих станций и серверов
Тема 4.2. Межсетевые экраны
Тема 4.3. IDS/IPS
Тема 4.4. VPN и криптографическая защита

Раздел 5. Безопасность информационных систем
Тема 5.1. Безопасность веб-приложений
Тема 5.2. OWASP Top 10
Тема 5.3. Безопасность облачных сервисов

Раздел 6. Управление инцидентами
Тема 6.1. Выявление инцидентов
Тема 6.2. Реагирование и расследование
Тема 6.3. SOC и SIEM

Раздел 7. Социальная инженерия

Тема 7.1. Фишинг и вишинг

Тема 7.2. Повышение осведомленности персонала

Раздел 8. Итоговый проект

Разработка концепции системы информационной безопасности организации

6. Практические занятия

1. Анализ угроз и построение модели угроз
2. Проведение оценки рисков
3. Настройка политик безопасности
4. Анализ инцидентов информационной безопасности
5. Разработка политики информационной безопасности организации
6. Защита итогового проекта

7. Фонд оценочных средств

7.1. Текущий контроль:

- тестирование
- выполнение практических заданий
- анализ кейсов

7.2. Итоговая аттестация:

- защита проекта по разработке системы информационной безопасности организации

8. Календарный учебный график

январь	•											
февраль		•										
март			•									
апрель				•								
май					•							
июнь						•						
июль							•					
август								•				
сентябрь									•			
октябрь										•		
ноябрь											•	
декабрь												•

9. Материально-техническое обеспечение

9.1. Учебная аудитория, мультимедийное оборудование, персональные компьютеры, доступ к сети Интернет, программные средства анализа защищенности и мониторинга событий безопасности.

10. Документы, выдаваемые по окончании прохождения (не прохождения) обучения

10.1. По окончании обучения, лицам, успешно прошедшим итоговую аттестацию, выдается удостоверение, подтверждающие прохождение обучения и/или повышение квалификации.

10.2. Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы, выдается справка об обучении.

10.3. Документ о повышении квалификации выдается на бланке, определяемом Обществом, оформленном на русском языке с проставлением печати, образец которого определяется и устанавливается Обществом самостоятельно.

11. Рекомендуемая литература

11.1. Основная литература:

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях
4. Девянин П.Н. Модели безопасности компьютерных систем
5. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации
6. Домарев В.В. Безопасность информационных технологий. Системный подход
7. Гафнер В.В. Информационная безопасность
8. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации

11.2. Нормативные документы:

1. Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»
3. ГОСТ Р ИСО/МЭК 27001-2021(национальный стандарт РФ – информационная технология, методы и средства обеспечения безопасности)
4. Приказы ФСТЭК России по защите информации.
5. Методические документы Банка России по кибербезопасности