**Межрегиональный центр профессионального развития**

**ООО ЦПП «ЗоргоСфера»**

1. **Паспорт Образовательной программы**

**«Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз»**

|  |  |
| --- | --- |
| **Версия программы** | 1 |
| **Дата Версии** | 09.01.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Общество с ограниченной ответственностью Центр подготовки персонала «ЗоргоСфера» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 3015105019 |
| 1.4 | Ответственный за программу | Емикова Елена Николаевна |
| 1.5 | Ответственный должность | директор |
| 1.6 | Ответственный Телефон | 8(8512)99-88-50 |
| 1.7 | Ответственный Е-mail | [education@uchzorgo.ru](mailto:education@uchzorgo.ru) |

1. **Основные данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз |
| 2.2 | Ссылка на страницу программы | [**общая характеристика программы**](#_ОБЩАЯ_ХАРАКТЕРИСТИКА_ПРОГРАММЫ) |
| 2.3 | Формат обучения | Онлайн |
| 2.4 | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Соглашение №1 «О совместном использовании информационного ресурса [www.do.uchzorgo.ru](http://www.do.uchzorgo.ru)» от 01.03.2019г. |
| 2.5 | Уровень сложности | Базовый |
| 2.6 | Количество академических часов | 72 |
| 2.7 | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 36 |
| 2.8 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | Стоимость: 30 000 рублей  <http://atcenter.ru/services/obuchenie-po-informatsionnoj-i-transportnoj-bezopasnosti/>  <https://www.cntiprogress.ru/seminarsforcolumn/37233.aspx>  <https://www.ed.cibit.ru/programmy-obucheniya/persdannie/>  Уникальность образовательной программы состоит в концепции перехода от традиционной модели «конфиденциальность, целостность, доступность» и регуляторной безопасности в сторону риск-ориентированной безопасности и защиты от внешних угроз. Смещение акцентов актуально, так как современные предприятия уязвимы перед атаками извне, которые могут влиять на показатели непрерывности бизнеса и деятельности организаций, а также общую доступность информационных систем и сервисов. |
| 2.9 | Минимальное количество человек на курсе | 1 |
| 2.10 | Максимальное количество человек на курсе | 200 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 21 |
| 2.12 | Формы аттестации | Тестирование |
| 2.13 | Указание на область реализации компетенций цифровой экономики | Кибербезопасность и защита данных |

1. **Аннотация программы**

Целью реализации программы повышения квалификации является совершенствование и (или) получение новых профессиональных компетенций, необходимых для выполнения следующих видов профессиональной деятельности в рамках имеющейся квалификации: формирование знаний, умений, навыков по обеспечению безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

К категории слушателей по данной программе относятся лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающее среднее и (или) высшее образование.

В результате освоения программы слушатель должен приобрести следующие знания и умения, необходимые для качественного изменения компетенций по проведению регламентных работ по эксплуатации систем защиты информации автоматизированных систем, ведению технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем, обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.

1. **ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА (ДПО)**

Титульный лист программы

Межрегиональный центр профессионального развития ООО ЦПП «ЗоргоСфера»

Дополнительная профессиональная программа повышения квалификации

«Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз»

72 час.

# ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

**1.Цель программы**

Совершенствование и (или) получение новых профессиональных компетенций, необходимых для выполнения следующих видов профессиональной деятельности в рамках имеющейся квалификации: формирование знаний, умений, навыков по обеспечению безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

**2.Планируемые результаты обучения:**

2.1.Знание

2.1.1.Обеспечения защиты информации при выводе из эксплуатации автоматизированных систем

2.1.2.Базовой конфигурации системы защиты информации автоматизированной системы

2.1.3.Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах

2.1.4.Типовых средств, методов и протоколов идентификации, аутентификации и авторизации

2.1.5.Нормативные правовые акты в области защиты информации

2.1.6.Организационных мер по защите информации

2.1.7.Основных методических и руководящих документов уполномоченных федеральных органов исполнительной власти по защите информации

2.1.8.Эксплуатационной и проектной документации на автоматизированную систему

2.1.9.Основных методов организации и проведения технического обслуживания технических средств информатизации

2.1.10.Процедуры по архивированию информации, обрабатываемой автоматизированной системой

2.1.11.Назначение и принципы работы основных узлов современных технических средств информатизации

2.1.12.Организацию ремонтного обслуживания компонентов автоматизированной системы

2.1.13.Регламент автоматизированной системы по уничтожению информации и машинных носителей информации

2.2. Умение

2.2.1.Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией

2.2.2.Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации

2.2.3.Производить монтаж и диагностику компьютерных сетей

2.2.4.Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи

2.2.5.Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации

2.2.6.Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации

2.2.7.Использовать программные средства для архивирования информации

2.2.8.Использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации

2.3.Навыки

2.3.1.Проверка работоспособности системы защиты информации автоматизированной системы

2.3.2.Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации

2.3.3.Контроль стабильности характеристик системы защиты информации автоматизированной системы

2.3.4.Ведение документов учета, обработки, хранения и передачи информации, составляющей тайну

2.3.5.Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации

2.3.6.Ведение протоколов и журналов учета при изменении конфигурации, осуществлении мониторинга и аудита систем защиты информации автоматизированных систем

2.3.7.Уничтожение информации и машинных носителей информации, архивирование информации, обрабатываемой автоматизированной системой

**3.Категория слушателей**

* 1. Лица, имеющие среднее профессиональное и (или) высшее образование

**4.Учебный план программы «Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Модуль 1 | 12 | 3 | 6 | 3 |
| 2 | Модуль 2 | 6 | 3 | - | 3 |
| 3 | Модуль 3 | 17 | 2 | 12 | 3 |
| 4 | Модуль 4 | 12 | 3 | 6 | 3 |
| 5 | Модуль 5 | 18 | 3 | 12 | 3 |
| 6 | Модуль 6 | 5 | 2 | - | 3 |
| **Итоговая аттестация** | | 2 | Тестирование | | |

**5.Календарный план-график реализации образовательной программы**

01.11.2020г. – 21.11.2020г.

02.11.2020г. – 22.11.2020г.

03.11.2020г. – 23.11.2020г.

04.11.2020г. – 24.11.2020г.

05.11.2020г. – 25.11.2020г.

Периодичность набора групп: 5 групп в месяц

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Модуль 1 | 12 | 01.11.– 04.11.2020 |
| 2 | Модуль 2 | 6 | 05.11.–06.11.2020 |
| 3 | Модуль 3 | 17 | 06.11.–11.11.2020 |
| 4 | Модуль 4 | 12 | 11.11.–14.11.2020 |
| 5 | Модуль 5 | 18 | 14.11.–20.11.2020 |
| 6 | Модуль 6 | 5 | 20.11.–21.11.2020 |
| 7 | Итоговая аттестация | 2 | 21.11.2020 |
| Всего: | | 72 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Модуль 1 | 12 | 02.11.– 05.11.2020 |
| 2 | Модуль 2 | 6 | 06.11.–07.11.2020 |
| 3 | Модуль 3 | 17 | 07.11.–12.11.2020 |
| 4 | Модуль 4 | 12 | 12.11.–15.11.2020 |
| 5 | Модуль 5 | 18 | 15.11.–21.11.2020 |
| 6 | Модуль 6 | 5 | 21.11.–22.11.2020 |
| 7 | Итоговая аттестация | 2 | 22.11.2020 |
| Всего: | | 72 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Модуль 1 | 12 | 03.11.– 06.11.2020 |
| 2 | Модуль 2 | 6 | 07.11.–08.11.2020 |
| 3 | Модуль 3 | 17 | 08.11.–13.11.2020 |
| 4 | Модуль 4 | 12 | 13.11.–16.11.2020 |
| 5 | Модуль 5 | 18 | 16.11.–22.11.2020 |
| 6 | Модуль 6 | 5 | 22.11.–23.11.2020 |
| 7 | Итоговая аттестация | 2 | 23.11.2020 |
| Всего: | | 72 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Модуль 1 | 12 | 04.11.– 07.11.2020 |
| 2 | Модуль 2 | 6 | 08.11.–09.11.2020 |
| 3 | Модуль 3 | 17 | 09.11.–14.11.2020 |
| 4 | Модуль 4 | 12 | 14.11.–17.11.2020 |
| 5 | Модуль 5 | 18 | 17.11.–23.11.2020 |
| 6 | Модуль 6 | 5 | 23.11.–24.11.2020 |
| 7 | Итоговая аттестация | 2 | 24.11.2020 |
| Всего: | | 72 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Модуль 1 | 12 | 05.11.– 08.11.2020 |
| 2 | Модуль 2 | 6 | 09.11.–10.11.2020 |
| 3 | Модуль 3 | 17 | 10.11.–15.11.2020 |
| 4 | Модуль 4 | 12 | 15.11.–18.11.2020 |
| 5 | Модуль 5 | 18 | 18.11.–24.11.2020 |
| 6 | Модуль 6 | 5 | 24.11.–25.11.2020 |
| 7 | Итоговая аттестация | 2 | 25.11.2020 |
| Всего: | | 72 |  |

**6.Учебно-тематический план программы «Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | **Источники, риски и формы атак на компьютерные системы** | **12** | **3** | **6** | **3** |  |
| 1.1 | Понятие информационной безопасности | 2 | 1 | - | 1 | тест |
| 1.2 | Стандартизация, сертификация и метрология как часть обеспечения информационной безопасности предприятия | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 1.3 | Управление уязвимостями информационной безопасности (ИБ) | 2 | 1 | - | 1 | тест |
| 2 | **Модели безопасности информационных систем** | **6** | **3** | **-** | **3** |  |
| 2.1 | Оценка рисков информационной безопасности | 2 | 1 | - | 1 | тест |
| 2.2 | Борьба с угрозами несанкционированного доступа к информации | 2 | 1 | - | 1 | тест |
| 2.3 | Защита критической информационной инфраструктуры | 2 | 1 | - | 1 | тест |
| 3 | **Стандарты безопасности. Законодательные меры защиты информации** | **17** | **2** | **12** | **3** |  |
| 3.1 | Стандарт ISO 27001 и способы его внедрения | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 3.2 | Информационная безопасность на производстве и в управлении качеством | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 3.3 | [Нормативные акты в области информационной безопасности в Российской Федерации](http://do.uchzorgo.ru/mod/resource/view.php?id=9879) | 1 | - | - | 1 | - |
| 4 | **Криптографические модели и методы защиты информации** | **12** | **3** | **6** | **3** |  |
| 4.1 | Криптографическая защита информации | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 4.2 | Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи | 2 | 1 | - | 1 | тест |
| 4.3 | Безопасность информации на мобильных устройствах | 2 | 1 | - | 1 | тест |
| 5 | **Защита информации с современных операционных системах** | **18** | **3** | **12** | **3** |  |
| 5.1 | Защита информации ограниченного доступа и предотвращение утечек информации | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 5.2 | Обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 1 | 6 | 1 | тест,  практическое задание |
| 5.3 | Безопасная разработка приложений в эпоху Agile | 2 | 1 | - | 1 | тест |
| 6 | **Защита информации в сети** | **5** | **2** | **-** | **3** |  |
| 6.1 | Безопасность компьютерных сетей | 2 | 1 | - | 1 | тест |
| 6.2 | Защита информации от утечки по техническим каналам | 2 | 1 | - | 1 | тест |
| 6.3 | [Виды информации, требующей защиты](http://do.uchzorgo.ru/mod/resource/view.php?id=9877) | 1 | - | - | 1 |  |
| 7 | **Итоговая аттестация** | 2 | - | - | 2 | тест |

**7. Учебная (рабочая) программа повышения квалификации «Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз»**

**Модуль 1 Источники, риски и формы атак на компьютерные системы (12 час.)**

Тема 1.1 Понятие информационной безопасности (2 час.)

Понятия и основные принципы ИБ, классификация методов обеспечения ИБ

Тема 1.2 Стандартизация, сертификация и метрология как часть обеспечения информационной безопасности предприятия (8 час.)

Обзор современных национальных и международных стандартов в области ИБ

Тема 1.3 Управление уязвимостями информационной безопасности (ИБ) (2 час.)

Система оценки уязвимостей, метрики оценки уявзимостей.

**Модуль 2 Модели безопасности информационных систем (6 час.)**

Тема 2.1 Оценка рисков информационной безопасности (2 час.)

Вопросы анализа рисков ИБ с возможность объективно оценить угрозы и распределить усилия и ресурсы для защиты от них.

Тема 2.2 Борьба с угрозами несанкционированного доступа к информации (2 час.)

Способы несанкционированного доступа к информации и методы его предотвращения

Тема 2.3 Защита критической информационной инфраструктуры (2 час.)

Безопасность критической информационной инфраструктуры (КИИ) в связи с принятием Федерального закона от 26.07.2017 187-ФЗ

**Модуль 3 Стандарты безопасности. Законодательные меры защиты информации (17 час.)**

Тема 3.1 Стандарт ISO 27001 и способы его внедрения (8 час.)

Действия организации для соответствия стандарту ISO 27001

Тема 3.2 Информационная безопасность на производстве и в управлении качеством (8 час.)

Вопросы обеспечения ИБ в промышленном производстве и управлении качеством

Тема 3.3 Нормативные акты в области информационной безопасности в Российской Федерации (1 час.)

Федеральные законы, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), критическая информационная инфраструктура

**Модуль 4 Криптографические модели и методы защиты информации (12 час.)**

Тема 4.1 Криптографическая защита информации (8 час.)

Понятие криптографии и методы криптографической защиты

Тема 4.2 Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи (8 час.)

Понятие электронной подписи, области ее применения и техническое обеспечение ее использования.

Тема 4.3 Безопасность информации на мобильных устройствах (2 час.)

Угрозы, подстерегающие пользователей мобильных устройств, и борьба с ними.

**Модуль 5 Защита информации с современных операционных системах (18 час.)**

Тема 5.1 Защита информации ограниченного доступа и предотвращение утечек информации (8 час.)

Защита информации ограниченного доступа, включая коммерческую тайну. Нормативная база, а также технические методы защиты информации компаний.

Тема 5.2 Обеспечение безопасности персональных данных при их обработке в информационных системах (8 час.)

Особенности обработки персональных данных в соответствии с законодательством Российской Федерации

Тема 5.3 Безопасная разработка приложений в эпоху Agile (2 час.)

Предотвращение инцидентов, связанных с неправильно написанным или сконфигурированным веб-приложе­нием, как способом получения злоумышленником данных о ее клиентах.

**Модуль 6 Защита информации в сети (5 час.)**

Тема 6.1 Безопасность компьютерных сетей (2 час.)

Устройства обеспечения сетевой безопасности, антивирусы, прокси-сервера, межсетевые экраны (МСЭ), NAC-решения, решения по защите от таргетированных атак и DDOS-атак. Их интеграция с другими средствами защиты информации (СЗИ)

Тема 6.2 Защита информации от утечки по техническим каналам (2 час.)

Способы несанкционированного доступа к информации и методы его предотвращения

Тема 6.3 Виды информации, требующей защиты (1 час.)

Информация, составляющая коммерческую тайну, банковская тайна (тайна банковских вкладов), служебная тайна, тайна кредитной истории, тайна страхования, тайна завещания, налоговая тайна, тайна усыновления ребенка, врачебная тайна и т.п.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1** | 1.2/1 | Исследование и анализ стандартов и спецификаций в организации | Проведение исследовательской работы в области метрологии, стандартизации и сертификации, с целью мониторинга соответствия системы обеспечения ИБ организации основным стандартам |
| **2** | 3.1/3 | Построение системы управления информационной безопасностью в организации | Определение достаточности принятых мер по уменьшению рисков ИБ в соответствии со стандартом |
| **3** | 3.2/3 | Составление проекта по приведению защиты АСУ ТП организации в соответствии с требованиями ФСТЭК | Разработать проект, учитывая три уровня управления АСУ ТП и предусмотреть внедрение СЗИ на каждом уровне |
| **4** | 4.1/4 | Изучение криптографических методов защиты информации | Шифрование и дешифрование информации методами криптографической защиты |
| **5** | 5.1/5 | Изучение способов защиты информации ограниченного доступа | Составление инструкции для оператора информационной системы, работа по внедрению режима коммерческой тайны в организации |
| **6** | 5.2/5 | Установка и настройка программного обеспечения VPN-клиент для Windows | Работа с VPN-клиент для Windows от установки до настройки и работы в системе |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |
| --- | --- |
| **№ модуля** | **Вопросы промежуточного тестирования** |
| 1 | Что относится к общедоступной информации в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07. 2006 № 149-ФЗ?  Что из перечисленного относится к конфиденциальной информации?  Что такое доступность информации?  Что такое подотчетность применительно к информационной безопасности?  В чьем ведении находится техническая защита информации, составляющей коммерческую тайну компании?  Какими бывают угрозы ИБ по характеру возникновения?  Какими бывают угрозы ИБ по типу злоумышленника?  Обязательны ли к применению стандарты по обеспечению ИБ?  Кто признается основоположником концепции, которая стала основой современного менеджмента и называется «Управление по целям»?  Какова основная цель стандартизации?  Какая структура в России является основным регулятором информационной безопасности?  Основным методом доказательства соответствия компании его требованиям стандарта является…  Какой из перечисленных стандартов регламентирует менеджмент рисков в области ИБ?  Программа обучения на рабочем месте, разработанная в США и затем использованная в Японии, получила название …  Что такое уязвимость в соответствии с ГОСТ Р 56546-2015?  Что такое организационная уязвимость?  Оценка опасности уязвимости CVSS имеет …. шкалу  Если уязвимость может быть эксплуатирована удаленно, то она …… той, которая может быть использована только локально  Какой вектор атаки является самым опасным?  Что из перечисленного дает возможность злоумышленникам проникнуть в сеть компаний и скомпрометировать информацию? |
| 2 | Основной международный стандарт в области ИБ ISO-27001 основан на оценке….  Существует два основных подхода к оценке рисков — …  При количественном анализе рисков ИБ формула SLE выглядит так: …  Что такое фактор воздействия при количественном анализе рисков ИБ?  Сколько существует способов обработки рисков ИБ?  Что подразумевает понятие «Передача риска»?  Сколько существует методик оценки рисков ИБ?  Для обеспечения правильной оценки рисков необходимо …  Дискреционный принцип управления доступом DAC – это …  Ролевой принцип управления доступом – это ...  Какая модель управления доступом является самой эффективной?  Возможен ли несанкционированный доступ к информации с использованием легитимного доступа к АС?  Что из перечисленного является предупреждающей мерой по защите информации от несанкционированного доступа?  Какая организационная мера может применяться для ИБ компании?  Оценка рисков бывает…  Критическая информационная инфраструктура (КИИ) – это …  Объекты критической информационной инфраструктуры – это …  Защита объектов КИИ осуществляется на основе присвоения им категорий значимости, исходя из факторов социальной, политической, экономической, экологической значимости или значимости для выполнения государственного оборонного заказа. Что подразумевается под политической значимостью?  Проект по приведению процессов и систем в соответствии с требованиями законодательства о КИИ состоит из … |
| 3 | В каком стандарте описываются процедуры мониторинга эффективности процессов управления ИБ?  В каком стандарте даны основы управления инцидентами ИБ?  Какой стандарт устанавливает требования к процессам управления ИБ?  Какого уровня управления (из перечисленных) нет в системе менеджмента компании?  Приемлемый уровень риска определяется ….  Как правило, организации управляют рисками на ... основе.  Документированная информация делится на …  Какова основная угроза безопасности АСУ ТП?  Как называются перехватчики-анализаторы трафика, которые позволяют находить уязвимости в программном обеспечении путем анализа заголовков пакетов?  Класс защищенности АСУ выбирается отдельно для каждого уровня и каждой системы, и может быть от К1 до К3, где К3 —…. класс.  Сколько существует уровней управления АСУ ТП? |
| 4 | Расшифруйте аббревиатуру СКЗИ.  Какие методы используются в криптографии?  Какое понятие применяется в полиалфавитных шрифтах?  Какой самый главный недостаток шрифта Виженера?  В каком из перечисленных шифров ключ является числом, повторяющимся столько раз, чтобы его длина равнялась длине оригинального текста?  Для шифрования и дешифрования в симметричном шифровании используется …  Что из перечисленного относится к методу перестановки?  Все симметричные шифры делятся на …  Что такое цифровая личность?  Для того, чтобы электронный документ имел юридическую силу, компания должна иметь …  Что такое электронная подпись?  Механизм электронной подписи использует криптосистему с открытым ключом, т.е. …  Какую информацию содержит сертификат открытого ключа?  Усиленная электронная подпись делится на …  Сертификаты электронной подписи записываются на специальные…  Какова основная составляющая в обеспечении безопасности информации?  С помощью какого документа регламентируется установка специального корпоративного ПО на личные мобильные телефоны сотрудников?  Что из перечисленного является задачей по обеспечению ИБ на мобильных устройствах?  Что такое фишинг?  Как называются сети зараженных компьютеров, в которые попадают устройства, на которых не установлены современные СЗИ? |
| 5 | Какого вида тайн НЕ существует согласно указу Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»?  Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить….  Каково назначение DLP-системы?  Как называется неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и получения защищаемой информации иностранными разведками?  Что такое коммерческая тайна?  Какие действия должен предпринять руководитель предприятия для защиты коммерческой тайны?  В каком году наша страна ратифицировала Европейскую конвенцию о защите прав человека и основных свобод?  Основным нормативным актом в Российской Федерации, регулирующим порядок обработки и защиты персональных данных, является….  Как дословно с английского переводится VPN (Virtual Private Network)?  Техническая защита конфиденциальной информации, в частности, проектирование в защищенном исполнении средств и систем информатизации, лицензируется ….  Если есть риск компрометации персональных данных при их передаче по открытым каналам связи, необходимо внедрять средства криптографической защиты информации, такая деятельность лицензируется …  На сколько типов делятся угрозы персональным данным?  Что из перечисленного входит в обязанности оператора персональных данных?  Какая ошибка является основной при написании кода ПО?  Какой из перечисленных видов анализа является статическим?  При выборе сканера статического анализа кода имеет смысл обращать внимание на ….  На какие виды делятся анализаторы кода? |
| 6 | Какая основная задача стоит перед администратором сети?  Как называется прокси-сервер, который дает доступ ко внутренним ресурсам локальной сети для внешних пользователей?  Сколько типов прокси-серверов существует?  Какого типа прокси-сервера НЕ существует?  Что из перечисленного является функцией SWG-решений, которая присутствует у основных решений, представленных на рынке?  Какова задача межсетевых экранов?  К основным видам устройств обеспечения сетевой безопасности относятся…  Какие каналы являются основными для получения нелегитимного доступа к информации?  Мощность электромагнитного излучения у старых мониторов была такой, что съем информации с них был возможен на расстоянии более километра, и с целью блокировки такой незаконной деятельности устанавливались специальные …  Как можно перехватывать речевую информацию по техническим каналам?  В акустических каналах для съема речевой информации, т.е. сигналов, передаваемых по воздуху, используются…  Какой метод используется в визуальных (видовых) каналах утечки данных?  Специальное обследование помещений предназначено для поиска в них…. |

**8.2. Обучающие задачи (кейсы):**

Разработать проект для эффективного внедрения системы управления информационной безопасностью в вашей организации, используя метод 8D.

Разработать проект построения системы управления информационной безопасностью в вашей организации, взяв за основу диаграмму Исикавы.

Разработать проект по приведению защиты АСУ ТП вашей организации, в соответствии с Приказом ФСТЭК России №31

Зашифровать, а затем дешифровать информацию с использованием методов перестановки, подстановки, шифром Вижинера

Разработка инструкции оператору информационной системы для защиты информации в соответствии с 149-ФЗ

Разработать проект по внедрению режима коммерческой тайны для вашей организации

**8.3. Критерии оценки тестирования:**

Менее 70% правильных ответов – оценка «неудовлетворительно»;

70% - 79% правильных ответов – оценка «удовлетворительно»;

80% - 89% правильных ответов – оценка «хорошо»;

90% - 100% правильных ответов – оценка «отлично».

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| 1 | Староверова Елена Львовна | ГБПОУ АО «АКВТ», преподаватель, высшая квалификационная категория, региональный эксперт WorldSkill Russia по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» | - |  | есть |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Словесные методы (самостоятельная работа), практические методы (практические занятия)  Электронное тестирование, лекции  Дистанционные обучающие технологии  Практико-ориентированный подход | Основная литература:  1 Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.  2 Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства Обеспечения информационной безопасности: учеб. пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.  3 Новиков В.К. Организационное информационной безопасности: В 2-х частях. Часть 1 Правовое обеспечение информационной безопасности: учеб. Пособие. – М.:МИЭТ,2013–184с.  4 Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013– 172 с.  Дополнительная литература:   1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006 Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г 2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/> 3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/> |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru  Информационно-справочная система по документам в области технической защиты информации www.fstec.ru  Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/  Справочно-правовая система «Консультант Плюс» www.consultant.ru  Справочно-правовая система «Гарант» [www.garant.ru](http://www.garant.ru)  Федеральный портал «Российское образование www.edu.ru | Система дистанционного обучения www.do.uchzorgo.ru, система видеоконференцсвязи Zoom |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Занятия с применением дистанционных образовательных технологий, итоговая аттестация | Компьютер, подключенный к сети Интернет; интернет-браузер; Adobe Flash Player; Adobe Reader, СДО [www.do.uchzorgo.ru](http://www.do.uchzorgo.ru) |

**III. Паспорт компетенций (Приложение 2)**

ПАСПОРТ КОМПЕТЕНЦИИ

Обеспечение риск-ориентированной информационной безопасности и защита от внешних угроз

(наименование дополнительной профессиональной образовательной программы повышения квалификации)

Общество с ограниченной ответственностью Центр подготовки персонала «ЗоргоСфера»

(наименование организации, реализующей дополнительную профессиональную образовательную программу повышения квалификации)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Основной целью программы формирования данной компетенции является подготовка слушателя к профессиональной деятельности, направленной на формирование готовности к обеспечению безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
| Знание:  - обеспечения защиты информации при выводе из эксплуатации автоматизированных систем  - базовой конфигурации системы защиты информации автоматизированной системы  - особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах  - типовых средств, методов и протоколов идентификации, аутентификации и авторизации  - нормативные правовые акты в области защиты информации  - организационных мер по защите информации  - основных методических и руководящих документов уполномоченных федеральных органов исполнительной власти по защите информации  - эксплуатационной и проектной документации на автоматизированную систему  - основных методов организации и проведения технического обслуживания технических средств информатизации  - процедуры по архивированию информации, обрабатываемой автоматизированной системой  - назначение и принципы работы основных узлов современных технических средств информатизации  - организацию ремонтного обслуживания компонентов автоматизированной системы  - регламент автоматизированной системы по уничтожению информации и машинных носителей информации  Умение :  - конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией  - обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации  -производить монтаж и диагностику компьютерных сетей  -использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи  -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  - использовать программные средства для архивирования информации  - использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации  Навыки  - проверка работоспособности системы защиты информации автоматизированной системы  - контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации  - контроль стабильности характеристик системы защиты информации автоматизированной системы  - ведение документов учета, обработки, хранения и передачи информации, составляющей тайну  - информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации  - ведение протоколов и журналов учета при изменении конфигурации, осуществлении мониторинга и аудита систем защиты информации автоматизированных систем  - уничтожение информации и машинных носителей информации, архивирование информации, обрабатываемой автоматизированной системой | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается) | 2 |
| Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | 3 |
| Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности) | 4 |
| Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | 5 |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция формируется во взаимосвязи с трудовыми функциями по проведению регламентных работ, ведение технической документации, обеспечение защиты информации при эксплуатации систем защиты информации автоматизированных систем | |
| 6. | Средства и технологии оценки | Электронное тестирование | |

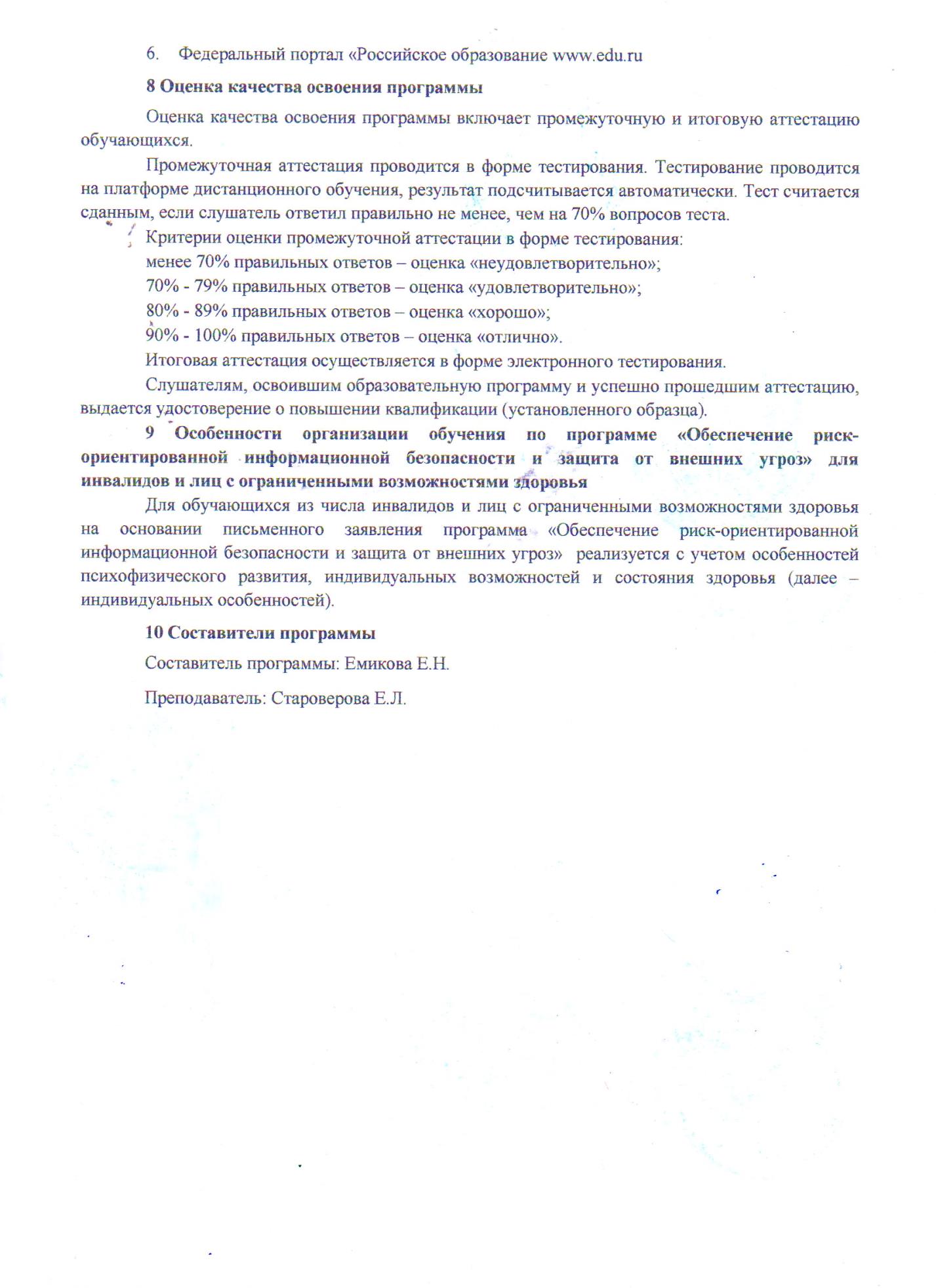
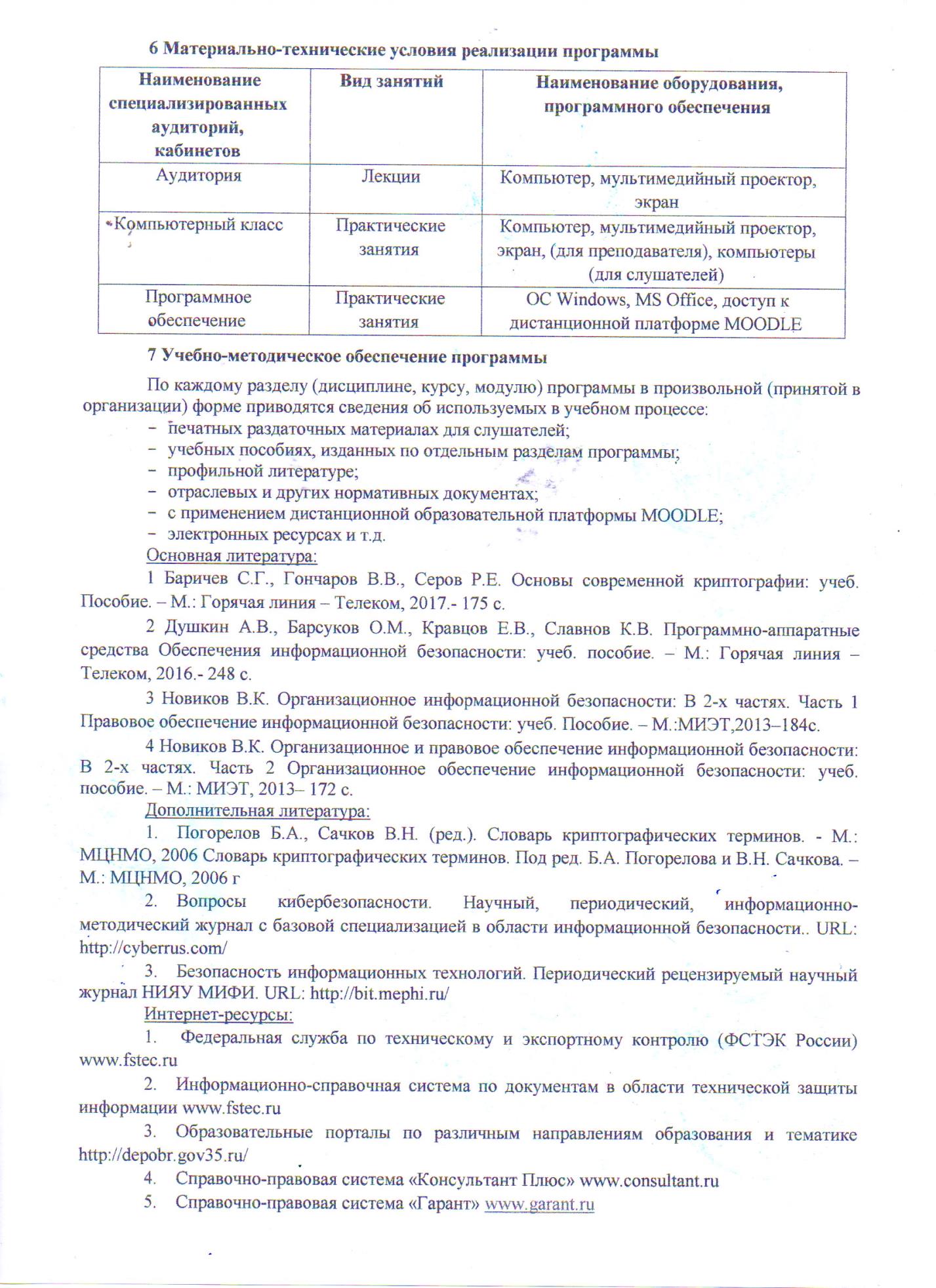
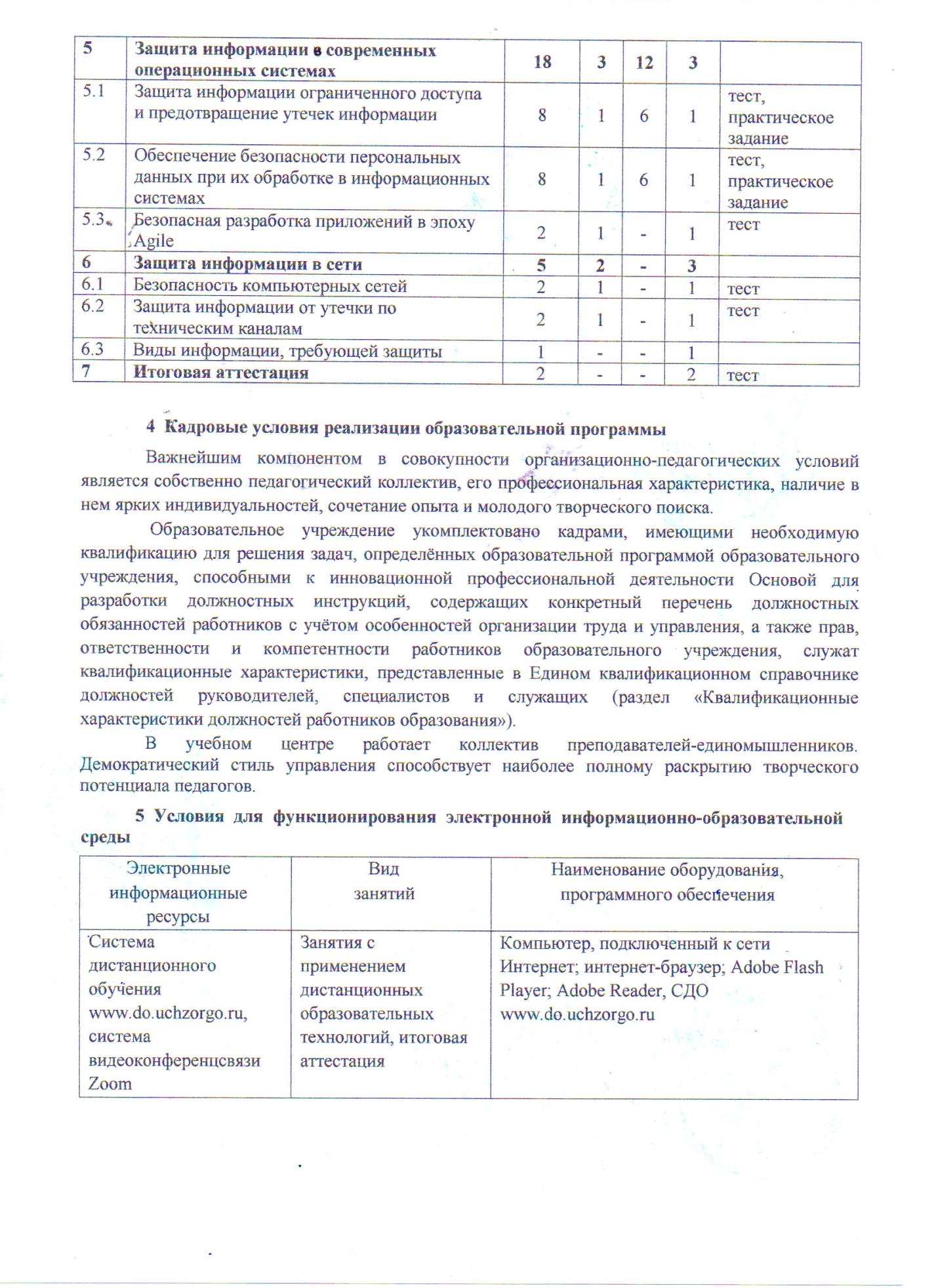
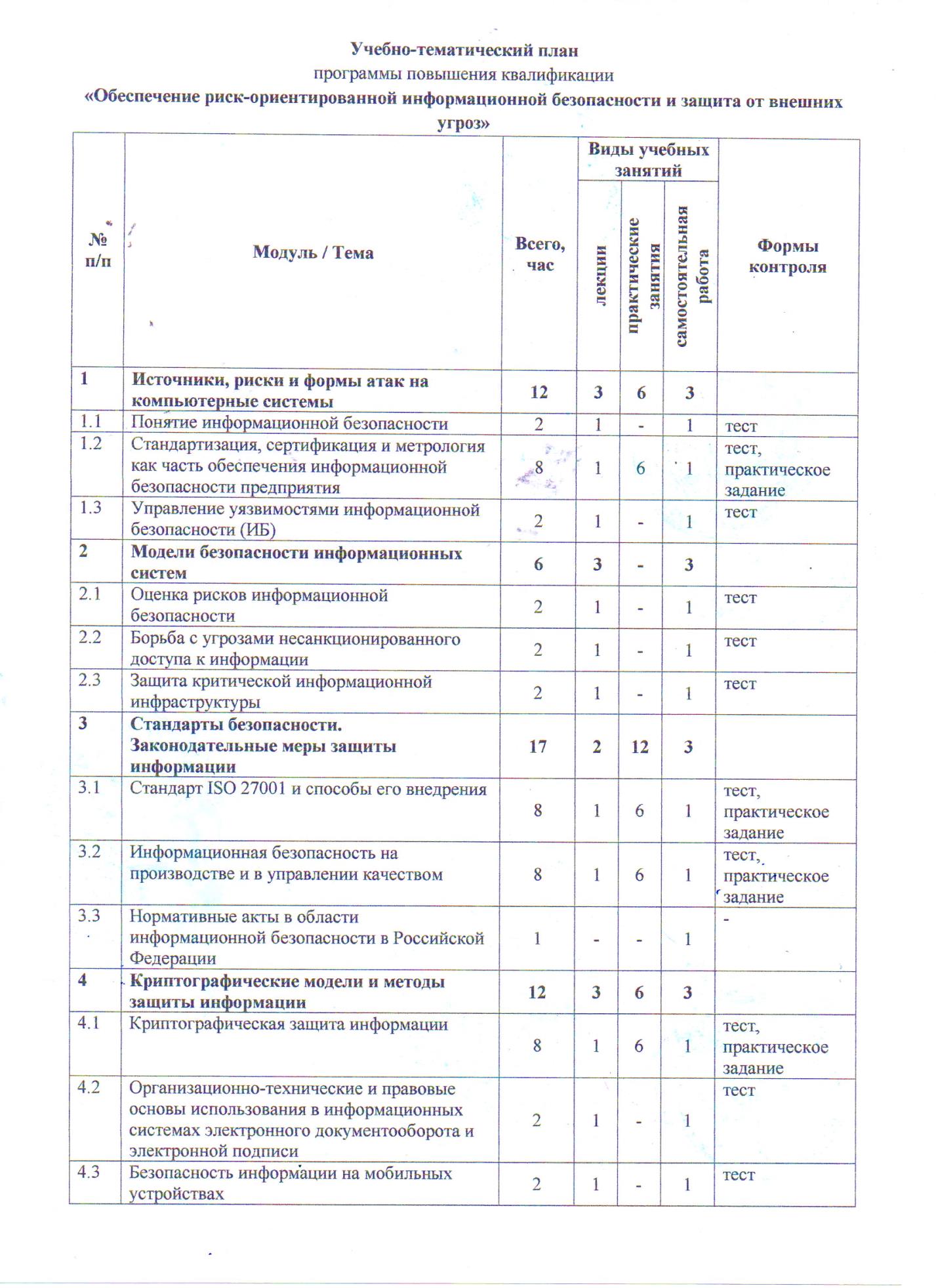
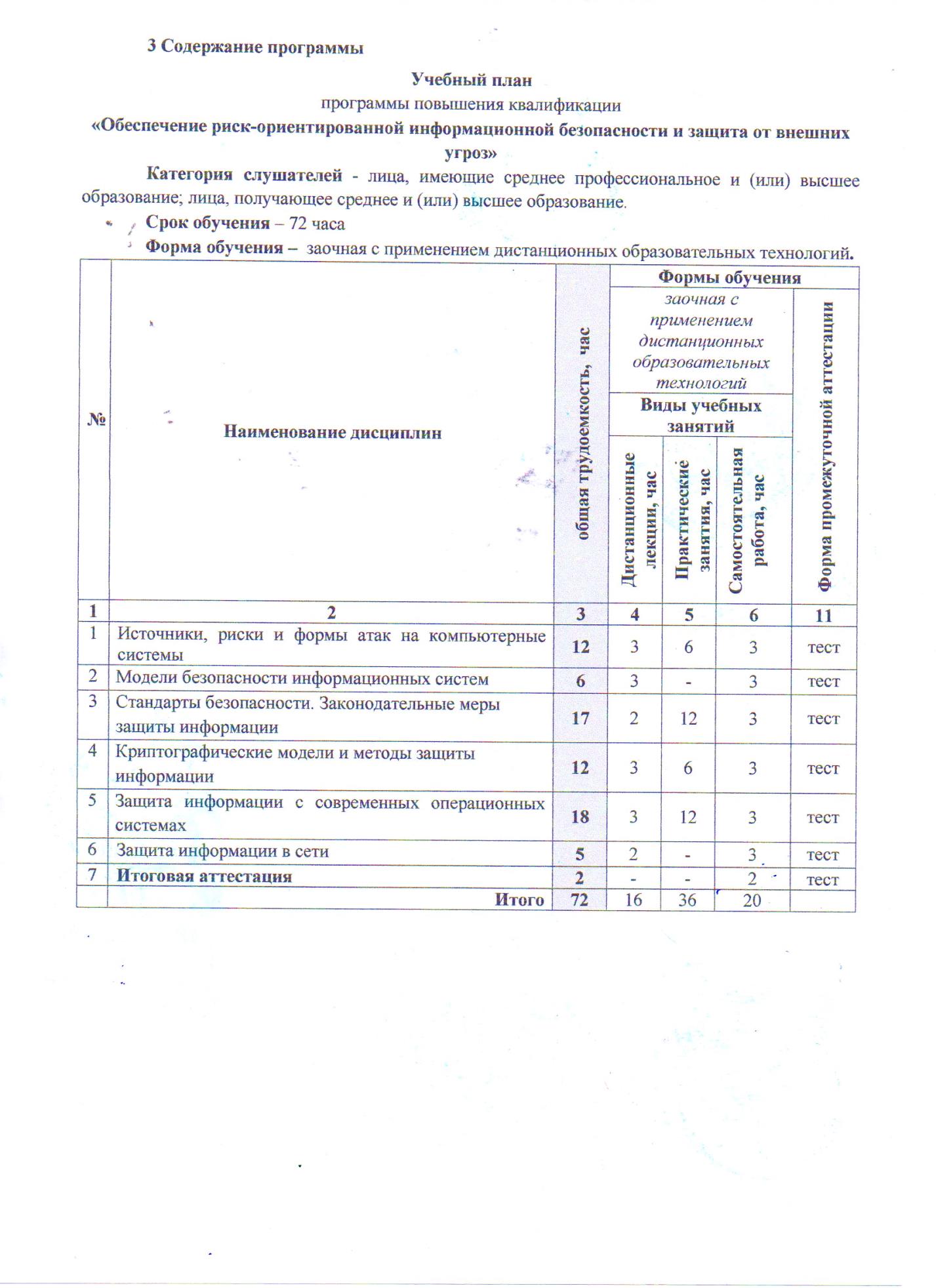
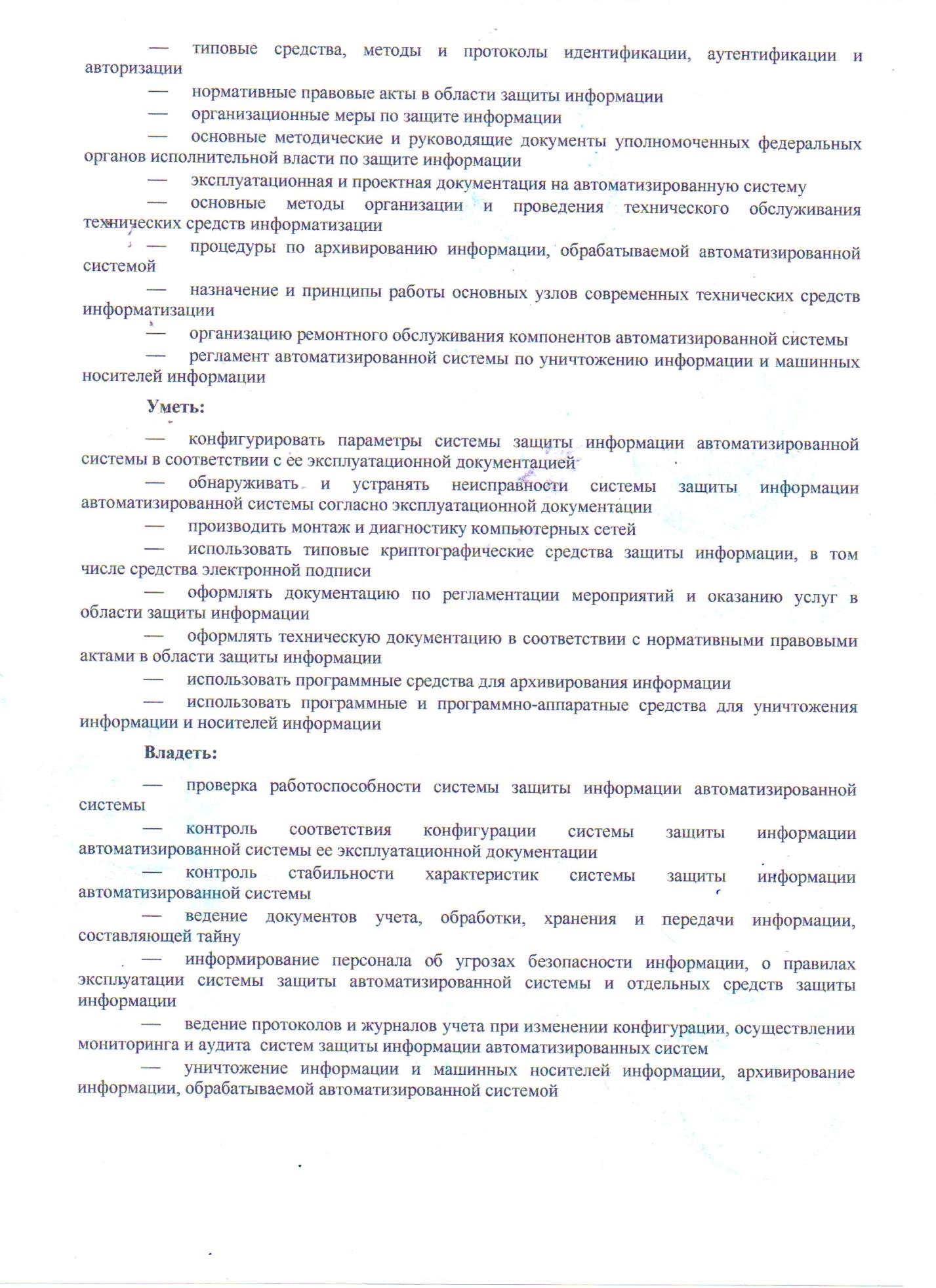
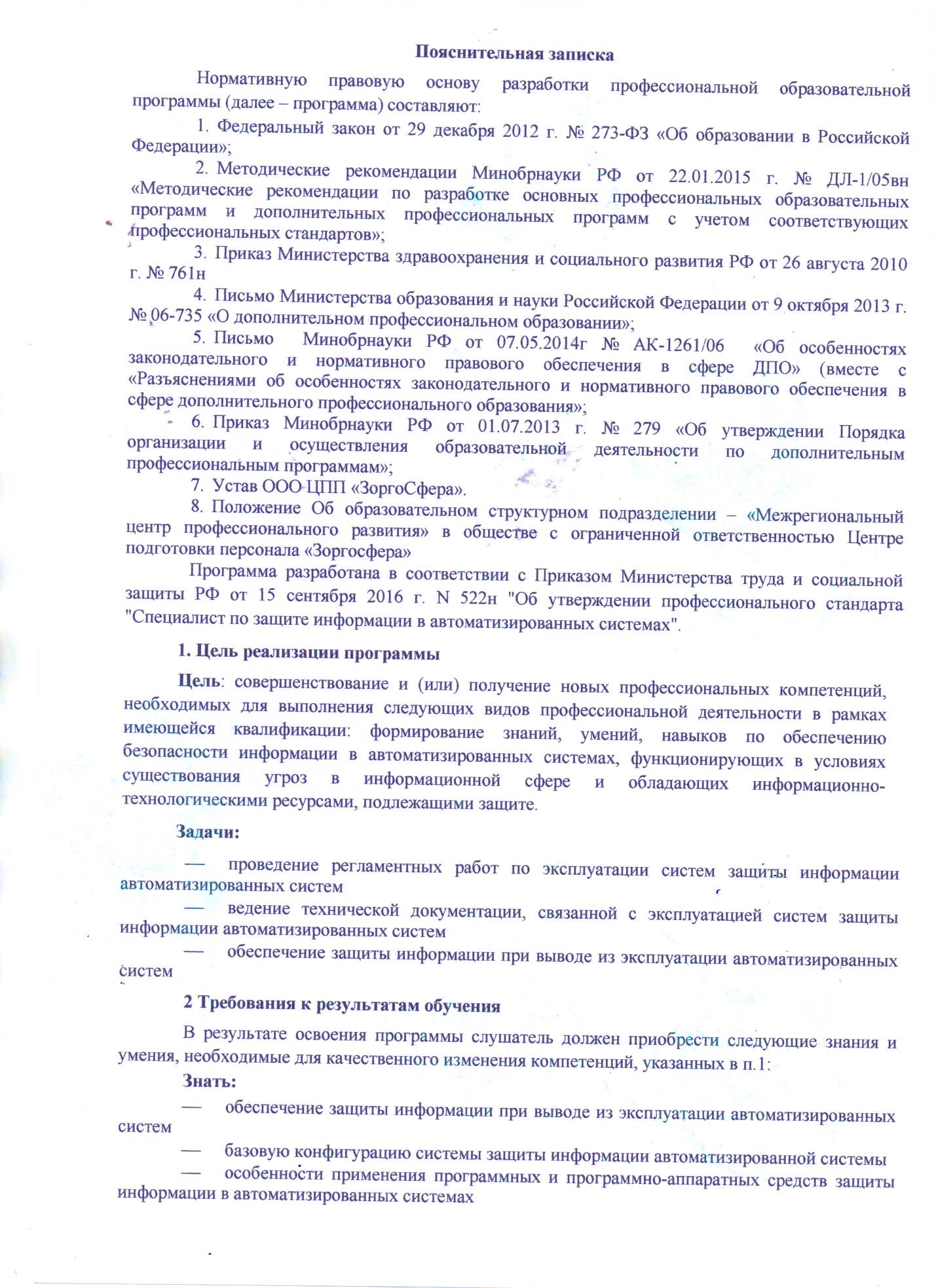
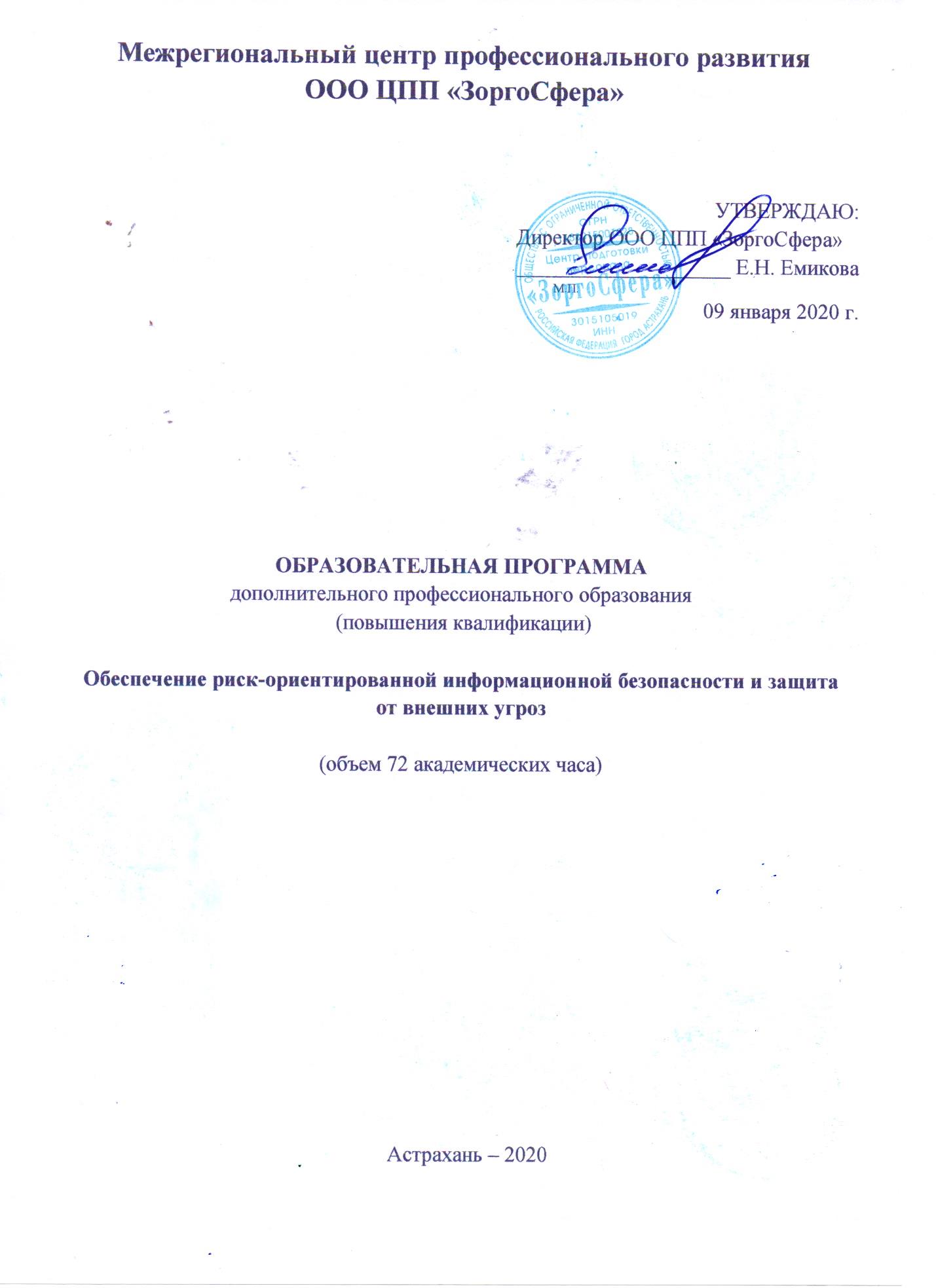
**VI.Иная информация о качестве и востребованности образовательной программы**

**V.Рекомендаций к программе от работодателей**: письма от работодателей

**VI.Указание на возможные сценарии профессиональной траектории граждан**: трудоустройство, развитие компетенций в текущей сфере занятости, переход в новую сферу занятости

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

****