Министерство образования и науки Астраханской области

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники»

Согласовано

Зам. директора по УМиВР

_____ С.В.Расторгуева

«12» ноября 2020 г.

Утверждаю

Директор колледжа

_____ Д.А.Лунев

«12» ноября 2020 г.

# Дополнительная профессиональная программа

# повышения квалификации

# «Обеспечение информационной безопасности при работе в сети»

**Аннотация программы повышения квалификации**

**Обеспечение информационной безопасности при работе в сети**

Программа дополнительного профессионального образования повышения квалификации разработана на основе:

Профессионального стандарта 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, утвержден приказом Министерства труда и социальной защиты Российской Федерации от 03.11.2016 № 608н

Программа дополнительного профессионального образования повышения квалификации Обеспечение информационной безопасности

при работе в сети предусматривает использование электронного обучения и дистанционных образовательных технологий.

Организация-разработчик:

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники» (ГБПОУ АО «АКВТ»).

Составители:

Староверова Е.Л., преподаватель дисциплин профессионального цикла ГБПОУ АО «АКВТ».

## 1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного профессионального образования – программы повышения квалификации «Обеспечение информационной безопасности при работе в сети» составляют:

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

Приказ Министерства образования и науки Российской Федерации от 23.08.2017 № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

Профессионального стандарта 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, утвержден приказом Министерства труда и социальной защиты Российской Федерации от 03.11.2016 № 608н

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование.

**Документ, выдаваемый после завершения обучения:** удостоверение о повышении квалификации.

## 2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

### 2.1. Цель реализации программы

Целью программы является обеспечение защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа к ним (НСД) в условиях существования угроз их информационной безопасности (ИБ), обеспечение сохранности персональных данных и другой конфиденциальной информации.

### 2.2. Планируемые результаты обучения

**Программа направлена на совершенствование**:

профессиональных компетенций :

- первичная настройка и проверка функционирования СССЭ;
- установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД;
-первичная настройка и проверка функционирования программных средств и систем защиты СССЭ от НСД;
- выявление угроз НСД к сетям электросвязи;
-сбор и систематизация (анализ и оценка) сведений об угрозах НСД к сетям электросвязи;
- оценка уязвимостей сетей электросвязи с точки зрения возможности НСД к ним;
- выработка предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи;
- контроль эффективности функционирования комплексной системы защиты сооружений и средств связи сетей связи специального назначения от НСД, включая выявление инцидентов, которые могут привести к сбоям или нарушению их функционирования или возникновению угроз безопасности информации, циркулирующей в них, а также реагирование на такие инциденты;
- анализ и оценка угроз НСД к сетям связи специального назначения;
- анализ и оценка работоспособности и эффективности применяемых программных средств защиты сетей связи специального назначения от НСД

| Обобщенные трудовые функции в соответствии с профессиональным стандартом 06.030 СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ | | |
|---|---|---|
| ТРУДОВАЯ ФУНКЦИЯ A5 Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД | | |
| Профессиональные компетенции на основании трудовых действий | Необходимые умения | Необходимые знания |
| A/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД | Проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НСД<br>Проводить монтаж (для программных средств - установку) СССЭ, средств и систем защиты СССЭ от НСД<br>Проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД | Номенклатура, функциональное назначение и основные характеристики СССЭ<br>Номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НСД<br>Нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НСД<br>Нормативные правовые акты в области связи, информатизации и защиты информации |
| ТРУДОВАЯ ФУНКЦИЯ D7 Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД | | |
| Профессиональные компетенции на основании трудовых действий | Необходимые умения | Необходимые знания |
| D/01.7 Анализ угроз информационной безопасности в сетях электросвязи | Выявлять и оценивать угрозы НСД к сетям электросвязи<br>Проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД | Модели угроз НСД к сетям электросвязи<br>Методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним<br>Средства анализа и контроля защищенности СССЭ<br>Нормативные правовые акты в области связи, информатизации и защиты информации<br>Национальные, межгосударственные и международные стандарты в области защиты информации |

| ТРУДОВАЯ ФУНКЦИЯ Е7 Обеспечение защиты средств связи сетей связи специального назначения от НСД | | |
|---|---|---|
| Профессиональные компетенции на основании трудовых действий | Необходимые умения | Необходимые знания |
| Е/01.7 Организация функционирования сетей связи специального назначения и их средств связи | Организовывать монтаж, настройку и эксплуатацию средств связи сетей связи специального назначения, средств и систем их защиты от НСД<br>Разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по обеспечению защиты сооружений и средств связи сетей связи специального назначения от НСД<br>Организовывать работы по выполнению требований режима защиты информации ограниченного доступа<br>Разрабатывать методические материалы и организационно-распорядительные документы по обеспечению защиты сооружений и средств связи сетей связи специального назначения от НСД | Модели угроз НСД к сооружениям и средствам связи сетей связи специального назначения<br>Нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования по защите информации сетей связи специального назначения |
| Е/03.7 Контроль защищенности от НСД и функциональности сетей связи специального назначения | Выявлять и оценивать угрозы НСД к сетям связи специального назначения<br>Проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей связи специального назначения от НСД<br>Разрабатывать предложения по нейтрализации угрозы НСД к сетям связи | Основные угрозы НСД и модели нарушителя политики информационной безопасности сетей связи специального назначения<br>Нормативные правовые акты по организации защиты государственной тайны и конфиденциальной информации<br>Способы и средства защиты информации от утечки по техническим каналам<br>Организационно-технические мероприятия по |

| | | |
|---|---|---|
| | специального назначения | защите сетей связи специального назначения от НСД и их эффективность<br>Нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к системам защиты сетей связи специального назначения и их средств связи от НСД |

**Программа направлена на приобретение новых профессиональных компетенций, необходимых для выполнения трудовых функций:**

| Трудовая функция с кодом | Профессиональные компетенции, обеспечивающие выполнение трудовой функции |
|---|---|
| ТРУДОВАЯ ФУНКЦИЯ A5<br>Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД | Первичная настройка и проверка функционирования СССЭ<br>Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД<br>Первичная настройка и проверка функционирования программных средств и систем защиты СССЭ от НСД |
| ТРУДОВАЯ ФУНКЦИЯ D7<br>Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД | Выявление угроз НСД к сетям электросвязи<br>Сбор и систематизация (анализ и оценка) сведений об угрозах НСД к сетям электросвязи<br>Оценка уязвимостей сетей электросвязи с точки зрения возможности НСД к ним<br>Выработка предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи |
| ТРУДОВАЯ ФУНКЦИЯ E7<br>Обеспечение защиты средств связи сетей связи специального назначения от НСД | Контроль эффективности функционирования комплексной системы защиты сооружений и средств связи сетей связи специального назначения от НСД, включая выявление инцидентов, которые могут привести к сбоям или нарушению их функционирования или возникновению угроз безопасности информации, циркулирующей в них, а также реагирование на такие инциденты<br>Анализ и оценка угроз НСД к сетям связи специального назначения<br>Анализ и оценка работоспособности и эффективности применяемых программных средств защиты сетей связи специального назначения от НСД |

**2.3. Объем программы (трудоемкость)**
Общая трудоемкость 72 академических часа, из них 60 аудиторных часов.

**2.4. Форма обучения**
Форма обучения – очная с использованием электронного обучения и дистанционных образовательных технологий

## 3. СОДЕРЖАНИЕ ПРОГРАММЫ

### 3.1. Учебный план и календарный учебный график

**Учебный план**
программы повышения квалификации
«Обеспечение информационной безопасности при работе в сети»

Категория слушателей:
Срок обучения – 72 час.
Форма обучения – очная

| Перечень учебных предметов, курсов, дисциплин (модулей), практик | Трудоемкость, часов | | | | Формы промежуточной аттестации, количество часов |
|---|---|---|---|---|---|
| | Всего | В том числе | | | |
| | | Лекции | Практические занятия | Самостоятельная работа | |
| Модуль 1. **Правовое обеспечение информационной безопасности при работе в сети** | 12 | 6 | 2 | | Семинар, 4ч |
| Модуль 2. **Обеспечение информационной безопасности при работе в корпоративной сети** | 56 | 18 | 22 | 12 | Семинар, 4ч |
| Итоговая аттестация | 4 | | | | Практическое задание, 4ч |
| Итого | 72 | | | | |

**Календарный учебный график**

| Перечень учебных предметов, курсов, дисциплин (модулей), практик | Учебные недели (дни)/нагрузка в часах | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Модуль 1. **Правовое обеспечение информационной безопасности при работе в сети** | 12 | | |
| Модуль 2. **Обеспечение информационной безопасности при работе в корпоративной сети** | 14 | 20 | 22 |
| Самостоятельная работа | | | 12 |
| Итоговая аттестация | | | 4 |

### 3.2. Рабочие программы модулей (курсов)

**Модуль 1. Правовое обеспечение информационной безопасности при работе в сети**

| Тема | Количество часов, всего | В том числе практические занятия |
|---|---|---|
| **Тема 1** Правовое обеспечение мероприятий по охране труда и технике безопасности в процессе | 2 | |

| | | |
|---|---|---|
| эксплуатации автоматизированных систем и средств защиты информации в них | | |
| **Тема 2** Понятие информации, защищаемой законодательством РФ | 2 | |
| **Тема 3** Основы законодательства РФ в области информационной безопасности и защиты информации<br>**Практическая работа:**<br>«Работа с автоматизированной информационно - поисковой системой. «Законодательная база РФ в области информационной безопасности и защите информации» | 4 | 2 |
| **Промежуточная** | 4 | 4 |

**Модуль 2. Обеспечение информационной безопасности при работе в корпоративной сети**

| Тема | Количество часов, всего | В том числе практические занятия |
|---|---|---|
| **Тема 1** Современная постановка задачи защиты информации | 2 | |
| **Тема 2** Информационные системы<br>**Практическая работа:**<br>«Классификация информационных систем» | 6 | 4 |
| **Тема 3** Угрозы информации<br>**Практическая работа:**<br>«Классификация угроз информации» | 4 | 2 |
| **Тема 4** Защита от компьютерных вирусов<br>**Практическая работа:**<br>«Разработка должностной инструкции техника по защите информации»<br>«Составления плана защиты информации» | 8 | 6 |
| **Тема 5** Методы и средства защиты компьютерной информации<br>**Практическая работа:**<br>«Разработка плана ограничения доступа» | 4 | 2 |
| Тема 6 Методические рекомендации для организации защиты информации при обработке персональных даниых<br>Практическая работа:<br>«Разработка соглашения на обработку персональных данных» | 6 | 2 |
| Тема 7 Защита информации от утечки по техническим каналам<br>**Практическая работа:**<br>«Использование технических средств для закрытия КНПИ»<br>«Составление акта использования технических средств для закрытия КНПИ» | 6 | 4 |
| **Тема 8** Обеспечение безопасности при работе в | 4 | 2 |

| | | |
|---|---|---|
| сети Интернет<br>**Практическая работа:**<br>«Составление памятки для пользователей сети Интернет» | | |
| **Самостоятельная работа** | 12 | 12 |
| **Промежуточная** | 4 | 4 |

**Модуль 1. Правовое обеспечение информационной безопасности при работе в сети**

**Тема 1 Правовое обеспечение мероприятий по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них**

Предмет и содержание курса, методы его изучения. Система организационно-правовой защиты информации как предмет изучения. Место организационной защиты информации в системе комплексной защиты информации организации (предприятия, учреждения, ведомства). Организационно-правовая защита информации как один из основных инструментов обеспечения безопасности организации.

**Тема 2 Понятие информации, защищаемой законодательством РФ**

Определение понятия – информация. Организационные формы представления информации. Развитие информационного законодательства. Классификация информации по роли, в которой она выступает в правовой системе. Классификация информации по доступу к ней. Юридические особенности и свойства информации

**Тема 3 Основы законодательства РФ в области информационной безопасности и защиты информации**

Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Другие законы и нормативные акты.

**Практическая работа:**

«Работа с автоматизированной информационно - поисковой системой. «Законодательная база РФ в области информационной безопасности и защите информации»

**Модуль 2. Обеспечение информационной безопасности при работе в корпоративной сети**

**Тема 1 Современная постановка задачи защиты информации (ДО)**

Организационно-правовое обеспечение информационной безопасности. Информация как объект юридической защиты. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в Российской Федерации

**Тема 2 Информационные системы (ДО)**

Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.

**Тема 3 Угрозы информации (ДО)**

Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь. Убытки, связанные с информационным обменом. Модель нарушителя информационных систем.

**Практическая работа: (ДО)**
«Классификация угроз информации»

**Тема 4 Защита от компьютерных вирусов (ДО)**
Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

**Практическая работа:**
«Разработка должностной инструкции техника по защите информации»

**Практическая работа:**
«Составления плана защиты информации»

**Тема 5 Методы и средства защиты компьютерной информации**
Классификация мер обеспечения безопасности компьютерных систем. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ.

**Практическая работа:**
«Разработка плана ограничения доступа»

**Тема 6 Методические рекомендации для организации защиты информации при обработке персональных данных**
Определения. Основные обязанности учреждений , эксплуатирующих ИСПДн, Основные мероприятия по приведению ИСПДн Учреждений в соответствие с ФЗ-152 "О персональных данных". Рекомендации по инвентаризации и категорированию персональных данных, обрабатываемых в ИСПДн Учреждений

**Практическая работа: (ДО)**
«Разработка соглашения на обработку персональных данных»

**Тема 7 Защита информации от утечки по техническим каналам (ДО)**
Понятие «утечка информации, канал связи». Источники утечки информации. Особенности утечки информации по каналам связи. Особенности используемых моделей перехвата. Основные каналы утечки информации. Алгоритм защиты каналов от утечки информации.

**Практическая работа: (ДО)**
«Использование технических средств для закрытия КНПИ»

**Практическая работа: (ДО)**
«Составление акта использования технических средств для закрытия КНПИ»

**Тема 8 Обеспечение безопасности при работе в сети Интернет (ДО)**
Угрозы сети Интернет, виды потерь, оценка потерь. Меры предотвращения угроз и защиты данных. Защита от соцсетей.

**Практическая работа: (ДО)**
«Составление памятки для пользователей сети Интернет»

**Самостоятельная работа**
- Творческое задание: «Разработка памятки начинающему пользователю ПК»
- Творческая работа: «Построение графика модели информационной сферы»
- Работа с нормативным документом: «Чтение текста первоисточника - Федеральный закон № 149-ФЗ от 23.07.2006 г. «Об информации, информационных технологиях и о защите информации»
- Работа с нормативным документом: «Проанализировать Конституцию Российской Федерации по закреплению прав и обязанностей субъектов по поводу подготовки (формирования), передачи и распространения документированной информации и информационных ресурсов, а также выдачи информации из информационных ресурсов потребителю»

**3.3. Оценочные материалы**

**Промежуточная аттестация**

**Семинар-круглый стол по модулю 1- подготовка к вопросам и обсуждение на темы:**

— Информационная безопасность в цифровую эпоху в коммерческих компаниях, деловой среде, государственном секторе.

— Цифровая среда доверия: изменяются ли приоритеты?

— Особенности формирования цифровой среды доверия в различных сферах.

— СМИ, фейковые новости – влияние на цифровую среду доверия.

— Надежная идентификация и аутентификация как условие формирования цифровой среды доверия.

— Регулирование и саморегулирование обеспечения информационной безопасности.

— Роль государства в формировании единой цифровой среды доверия.

— Юридически значимый электронный документооборот.

**Семинар-круглый стол по модулю 2- подготовка к вопросам и обсуждение на тему «Безопасность в сети Интернет»**

Задачи:

познакомиться:

-с правилами ответственного и безопасного поведения в современной информационной среде;

- способах защиты от противоправных посягательств в сети Интернет;

Как критически относиться к сообщениям в СМИ (в т.ч. электронных);

- как отличить достоверные сведения от недостоверных, как избежать вредной и опасной информации, как распознать признаки злоупотребления доверчивостью и сделать более безопасным свое общение в сети Интернет;

- как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Форма круглого стола: дискуссия с элементами ролевой игры.

-повышение осведомленности детей о позитивном контенте сети Интернет, полезных возможностях глобальной сети для образования, развития, общения; - повышение уровня осведомленности детей о проблемах безопасности при использовании детьми сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.

**Итоговая аттестация – 4 часа**

Итоговая аттестация проводится в форме практической работы по составлению и заполнению пакета документации для обеспечения защиты данных сети по варианту согласно месту работы слушателя

**Критерии оценки знаний слушателей**

В процессе итоговой аттестации слушатель должен продемонстрировать:

- грамотный анализ предметной области;
- владение навыками работы с нормативными правовыми актами;
- владение методами формирования требований по защите информации;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- использование нормативных правовых актов в области защиты информации;
- использование организационных мер по защите информации.

## 4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

### 4.1. Материально-технические условия реализации программы

Предполагает использование мастерской «Корпоративная защита от внутренних угроз информационной безопасности»

Оборудование:

- рабочие места на базе вычислительной техники, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет»;
- аудиовизуальный комплекс

### 4.2. Учебно-методическое и информационное обеспечение.

1. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с.— Режим доступа: http://www.iprbookshop.ru/1 2014.— ЭБС «IPRbooks», по паролю

2. Методический документ "Меры защиты информации в государственных информационных системах" (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.). http://fstec.ru/component/attachments/download/675 (дата обращения 21.03.2017)

3. Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий" (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19 июня 2002 г. N 187). http://fstec.ru/component/attachments/download/293 (дата обращения 21.03.2017)

4. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2010.— 328 с.

5. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006). http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty (дата обращения 21.03.2017)

6. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005). http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty (дата обращения 21.03.2017)

7. Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных». http://fstec.ru/component/finder/search (дата обращения 21.03.2017)

8. Федеральный закон Российской Федерации № 149-ФЗ «Об информации, информационных технологиях и о защите информации». http://fstec.ru/component/finder/ (Дата обращения 21.03.2017)

9. Каталог по безопасности www.sec.ru/

10. Компьютерная безопасность www.bugtraq.ru/

11. Сайт Федеральной Службы Безопасности http://www.fsb.ru/

12. ФСТЭК России http://fstec.ru/

13. Лаборатория Касперского http://www.kaspersky.ru/

14. Сайты ассоциаций, консорциумов, институтов и других исследовательских организаций, занимающихся разработкой стандартов, средств защиты информации, образовательных программ и т.п. http://www.iso27000.ru/katalog-ssylok/associacii-i-konsorciumy/

15. Институт специалистов по компьютерной безопасности SANS - одна из наиболее авторитетных организаций в области компьютерной безопасности. Еженедельный обзор последних уязвимостей http://www.sans.org/

**4.3. Кадровое обеспечение программы**

| № п/п | ФИО | Статус в экспертном сообществе Ворлдскиллс с указанием компетенции | Должность, наименование организации |
|---|---|---|---|
| 1 | Староверова Елена Львовна | Региональный эксперт в компетенции «Корпоративная защита от внутренних угроз информационной безопасности» | Преподаватель ГБПОУ АО «Астраханский колледж вычислительной техники», преподаватель специальных дисциплин |
| 2 | Семернева Наталья Викторовна | Эксперт с правом оценки демонстрационного экзамена по компетенции «Разработка мобильных приложений» | Преподаватель ГБПОУ АО «Астраханский колледж вычислительной техники», преподаватель специальных дисциплин |