Дополнительная профессиональная программа повышения квалификации **«Защита программ и данных»** (далее − программа) подготовлена на основе:

− Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации;

− требований Приказа Минобрнауки России от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

− методических рекомендаций-разъяснений Минобрнауки России по разработке дополнительных профессиональных программ на основе профессиональных стандартов от 22 апреля 2015 года № ВК-1030/06;

− требований Приказа Министерства науки и высшего образования Российской Федерации от 19.10.2020 № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

Реализация программы направлена на совершенствование имеющихся и/или получение новых компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации.

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения, определен приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (зарегистрировано в Минюсте России 28 сентября 2016 г., № 43857, регистрационный номер 843).

**Цель программы** – теоретическая и практическая подготовка программных реализаций, направленных на защиту программ и программных систем от анализа и вредоносных программных воздействий.

**Задачи программы –** изучить средства и методы анализа программных реализаций, защиты программ от анализа, выявления программных закладок; модели функционирования и методы внедрения программных закладок.

**Категория обучающихся** – для освоения ДПП допускаются лица, имеющие высшее образование уровня специалитет или магистратура в области информационной безопасности и/или освоившие дополнительное профессиональное образование в области информационной безопасности и имеющие практические навыки в данной области.

**Форма обучения** – очная, возможно использование дистанционных образовательных технологий.

**Трудоемкость обучения** – 48 общих часов, из них 32 часов аудиторной работы и 16 часов самостоятельной работы.

Слушатели изучат безопасное (защищенное) программное обеспечение, уязвимости веб-приложений, жизненный цикл разработки безопасного программного обеспечения, моделирование угроз безопасности информации.

Программа реализуется одним модулем, включающим две темы:

**1. Типовые уязвимости программного обеспечения и меры защиты от них:** Безопасность веб-приложений: SOP, cookie, идентификация, аутентификация, авторизация. Уязвимости веб-приложений.

**2. Жизненный цикл разработки безопасного программного обеспечения:** основные понятия, термины и определения. Тестирование проникновения при разработке безопасного программного обеспечения.

Итоговая аттестация проводится в форме зачета. Лицам, успешно прошедшим обучение и выполнившим контрольные мероприятия, предусмотренные программой, выдается удостоверение о повышении квалификации.