Описание программы профессиональной переподготовки

**«Информационная безопасность. Безопасность значимых объектов критической информационной инфраструктуры» 502 часа**

* **Программа согласована с ФСТЭК России**
* **Программа профессиональной переподготовки разработана на основании:**
* примерной программы ФСТЭК России «Информационная безопасность. Безопасность значимых объектов критической информационной» (разработанной и утвержденной ФСТЭК России 30 июня 2023 г.);
* профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 9 августа 2022 г. № 474н;
* профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 536н;
* профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 533н;
* профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 14 сентября 2022 г. № 525н;
* федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26 ноября 2020 г. № 1457.
* **Целью реализации программы** профессиональной переподготовки является формирование компетенций, необходимых специалистам (включая государственных гражданских служащих) для выполнения нового вида профессиональной деятельности «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».
* **Аннотация**

1 мая 2022 года президент России Владимир Путин подписал указ № 250, направленный на обеспечение информационной безопасности ряда ключевых органов и организаций России, в их числе – субъектов критической информационной инфраструктуры (далее - КИИ).

В соответствии с требованиями Указа, в целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации руководителям вышеперечисленных органов и организаций необходимо иметь в штате сотрудников, обладающих необходимым уровнем компетенций и обеспечивающих информационную безопасность органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Задачей этих сотрудников является построение системы информационной безопасности органа (организации) и обеспечение ее функционирования на всем этапе жизненного цикла объектов критической информационной инфраструктуры, а также непрерывное улучшение данной системы и контроль выполнения требований нормативно-правовых актов Российской Федерации при проведении данных работ.

Дополнительно требования к квалификации руководителя и сотрудников подразделения, обеспечивающего безопасность значимых объектов КИИ, установлены Приказом ФСТЭК России от 11 декабря 2017 г. № 235.

* **Категории обучающихся**

Программа ориентирована на переподготовку:

* Заместителя руководителя органа (организации), ответственного за обеспечение информационной безопасности;
* Руководителя структурного подразделения, обеспечивающего безопасность значимых объектов КИИ;
* Специалистов, работающих в области обеспечения кибербезопасности значимых объектов КИИ.
* **Необходимая подготовка**

К освоению программы допускаются лица, имеющие *высшее образование* по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Минобрнауки России.

* Успешное окончание обучения по программе курса позволит специалистам:
* применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность в области обеспечения безопасности значимых объектов КИИ в своей профессиональной деятельности;
* определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;
* планировать создание и развитие систем безопасности значимых объектов КИИ;
* организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами и методическими документами ФСБ России, ФСТЭК России;
* планировать, разрабатывать и реализовывать меры по обеспечению безопасности значимых объектов КИИ;
* выявлять объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
* формировать перечень объектов КИИ и присваивать категории значимости объектов КИИ;
* разрабатывать техническое задание на создание значимого объекта КИИ и (или) техническое задание на подсистему безопасности значимого объекта КИИ;
* информировать и обучать персонал значимого объекта КИИ;
* проводить анализ угроз безопасности информации в отношении значимых объектов КИИ и выявление уязвимостей в них;
* разрабатывать модель угроз безопасности информации значимого объекта КИИ или ее уточнение (при ее наличии);
* формировать требования к организационным и техническим мерам,
* применяемым для обеспечения безопасности значимого объекта КИИ;
* обеспечивать функционирование систем безопасности значимых объектов КИИ;
* взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и с Национальным координационным центром по компьютерным инцидентам (НКЦКИ);
* определять актуальные угрозы безопасности информации на основе анализа банка данных угроз безопасности информации ФСТЭК России в значимом объекте КИИ и их нейтрализацию;
* осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;
* реагировать на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ;
* проводить контроль за обеспечением безопасности значимого объекта КИИ.
* **Освоившие программу специалисты будут:**

**Знать:**

* нормативные правовые акты, методические документы и национальные стандарты в области информационной безопасности и обеспечения безопасности значимых объектов КИИ;
* основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами значимых объектов КИИ;
* задачи и полномочия подразделения по защите информации; основы построения систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования;
* процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;
* общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования;
* типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;
* особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах;
* архитектуру современных операционных систем, применяемых в автоматизированных системах управления и информационных системах;
* основы взаимодействия субъектов КИИ с ФСТЭК и ГосСОПКА;
* организационные и технические основы построения систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования;
* основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности;
* порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ;
* порядок организации и проведения работ по аттестации объектов информатизации (значимых объектов КИИ Российской Федерации) по требованиям о защите информации ограниченного доступа, не составляющей государственную тайну;
* порядок и содержание работ по анализу уязвимостей программных и программно-аппаратных средств;
* меры по восстановлению функционирования и проверке работоспособности значимого объекта КИИ в ходе ликвидации последствий компьютерных атак.

**Уметь:**

* применять нормативную базу в области обеспечения безопасности информации;
* анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации;
* определять категории значимости объектов КИИ и формировать акт, содержащий сведения об объекте КИИ, сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;
* разрабатывать организационно-распорядительные документы по безопасности значимых объектов КИИ;
* определять требования к обеспечению безопасности значимого объекта КИИ;
* разрабатывать модели угроз безопасности информации значимых объектов КИИ по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации, анализа банка данных угроз безопасности информации;
* определять политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
* устанавливать, настраивать и использовать программные средства системного и прикладного назначения;
* осуществлять выбор средств защиты информации и (или) их разработку с учетом категории значимости значимого объекта КИИ, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
* определять меры по обеспечению безопасности при взаимодействии значимого объекта КИИ с иными объектами КИИ, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями;
* осуществлять внедрение подсистемы безопасности значимого объекта КИИ;
* осуществлять контроль обеспечения безопасности значимого объекта КИИ;
* оформлять документы, представляемые в орган по аттестации при проведении работ по аттестации объектов информатизации;
* определять актуальные угрозы безопасности информации;
* проводить испытания значимого объекта КИИ и его подсистемы безопасности.
* **Владеть навыками, выполнять следующие трудовые действия:**
* работа с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ;
* разработка организационно-распорядительных документов по безопасности значимых объектов КИИ;
* внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ и ввод его в действие;
* установка, настройка и использование программных средств системного и прикладного назначения, управление программным обеспечением;
* планирование мероприятий по обеспечению безопасности значимого объекта КИИ;
* анализ угроз безопасности информации в значимом объекте КИИ и последствий от их реализации;
* реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ;
* информирование и обучение персонала значимого объекта КИИ;
* контроль за обеспечением безопасности значимого объекта КИИ;
* оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.