МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

(Минтруд России)

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Москва
Регистрационный № 88334
от "18" сентября 2026.

ПРИКАЗ

14 августа 2026 г. № 352н

Об утверждении профессионального стандарта «Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры»

В соответствии с пунктом 20 Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 10 апреля 2023 г. № 580, п р и к а з ы в а ю:

1. Утвердить прилагаемый профессиональный стандарт «Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры».

2. Установить, что настоящий приказ вступает в силу с 1 марта 2027 г. и действует до 1 марта 2033 г.

Министр А.О. Котяков

УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от «7» августа 2026 г. № 352н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры

1779
Регистрационный номер

Содержание

I. Общие сведения 1
II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности) 3
III. Характеристика обобщенных трудовых функций 6
3.1. Обобщенная трудовая функция «Обеспечение функционирования средств защиты информации значимых объектов критической информационной инфраструктуры» 6
3.2. Обобщенная трудовая функция «Реализация средствами защиты информации требований обеспечения безопасности значимых объектов критической информационной инфраструктуры» 9
3.3. Обобщенная трудовая функция «Обнаружение компьютерных атак и реагирование на инциденты на значимых объектах критической информационной инфраструктуры» 13
3.4. Обобщенная трудовая функция «Разработка подсистемы безопасности значимых объектов критической информационной инфраструктуры» 17
3.5. Обобщенная трудовая функция «Контроль обнаружения компьютерных атак и реагирования на инциденты на значимых объектах критической информационной инфраструктуры» 22
3.6. Обобщенная трудовая функция «Управление обеспечением безопасности значимых объектов критической информационной инфраструктуры» 26
IV. Сведения об организациях – разработчиках профессионального стандарта 31
V. Сокращения, используемые в профессиональном стандарте 31

I. Общие сведения

Обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры	06.057
(наименование вида профессиональной деятельности)	код

Краткое описание вида профессиональной деятельности

Обеспечение безопасности значимых объектов критической информационной инфраструктуры в целях их устойчивого функционирования при проведении в отношении них компьютерных атак и реализации угроз безопасности информации

Группа занятий

1213	Руководители в области определения политики и	1330	Руководители служб и подразделений в сфере

	планирования деятельности		информационно-коммуникационных технологий
2529	Специалисты по базам данных и сетям, не входящие в другие группы	3513	Специалисты-техники по компьютерным сетям и системам
(код ОКЗ[1])	(наименование)	(код ОКЗ)	(наименование)

Отнесение к области профессиональной деятельности

06	Связь, информационные и коммуникационные технологии
(код ОПД[2])	(наименование области профессиональной деятельности)

Отнесение к видам экономической деятельности

62.09	Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая
74.90.93	Деятельность по мониторингу информационной безопасности средств и систем информатизации
74.90.94	Деятельность по обеспечению защиты информации
(код ОКВЭД[3])	(наименование вида экономической деятельности)

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции				Трудовые функции		
код	Наименование	уровень квалификации	возможные наименования должностей, профессий рабочих	наименование	код	уровень (подуровень) квалификации
A	Обеспечение функционирования средств защиты информации значимых объектов критической информационной инфраструктуры	5	Техник по защите информации Техник по безопасности компьютерных систем и сетей Специалист по взаимодействию с персоналом и пользователями центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Специалист по обнаружению компьютерных атак и инцидентов центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	Установка, настройка и техническое обслуживание средств защиты информации значимых объектов критической информационной инфраструктуры	A/01.5	5
				Обеспечение работоспособности средств защиты информации значимых объектов критической информационной инфраструктуры	A/02.5	5
				Регистрация событий и инцидентов информационной безопасности	A/03.5	5
B	Реализация средствами защиты информации требований обеспечения безопасности значимых объектов	6	Специалист по защите информации в компьютерных системах и сетях Специалист по информационной безопасности	Управление уязвимостями значимых объектов критической информационной инфраструктуры	B/01.6	6
				Определение порядка, реализация и контроль выполнения средствами защиты информации требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической	B/02.6	6

	критической информационной инфраструктуры			информационной инфраструктуры		
				Администрирование средств (управление средствами) защиты информации значимых объектов критической информационной инфраструктуры	B/03.6	6
C	Обнаружение компьютерных атак и реагирование на инциденты на значимых объектах критической информационной инфраструктуры	6	Инженер информационно-аналитического подразделения Специалист по ликвидации последствий компьютерных инцидентов Специалист по установлению причин компьютерных инцидентов Аналитик центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение фактов компьютерных атак	C/01.6	6
				Реагирование на инциденты информационной безопасности	C/02.6	6
				Апостериорный анализ инцидентов информационной безопасности	C/03.6	6
D	Разработка подсистемы безопасности значимых объектов критической информационной инфраструктуры	7	Ведущий инженер – разработчик систем защиты информации Ведущий специалист по защите информации Главный специалист по защите информации Руководитель проектов в области разработки систем защиты информации Начальник отдела (лаборатории, сектора) защиты информации Руководитель структурного подразделения по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Категорирование объектов критической информационной инфраструктуры	D/01.7	7
				Разработка требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры	D/02.7	7
				Проектирование и реализация подсистемы безопасности значимых объектов критической информационной инфраструктуры	D/03.7	7
				Аудит информационной безопасности значимых объектов критической информационной инфраструктуры	D/04.7	7

E	Контроль обнаружения компьютерных атак и реагирования на инциденты на значимых объектах критической информационной инфраструктуры	7	Ведущий специалист по защите информации Начальник направления центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Заместитель руководителя центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Руководитель центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	Контроль анализа и обработки компьютерных инцидентов на значимых объектах критической информационной инфраструктуры	E/01.7	7
				Организация расследования компьютерных инцидентов на значимых объектах критической информационной инфраструктуры	E/02.7	7
				Контроль апостериорного анализа компьютерных инцидентов	E/03.7	7
F	Управление обеспечением безопасности значимых объектов критической информационной инфраструктуры	8	Директор по развитию цифровых технологий документированных сфер деятельности организации Заместитель генерального директора по информационной безопасности	Определение измеримых и практических результатов деятельности по обеспечению безопасности значимых объектов критической информационной инфраструктуры	F/01.8	8
				Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов критической информационной инфраструктуры	F/02.8	8
				Организация мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры	F/03.8	8

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Обеспечение функционирования средств защиты информации значимых объектов критической информационной инфраструктуры	Код	A	Уровень квалификации	5

Возможные наименования должностей, профессий рабочих	Техник по защите информации Техник по безопасности компьютерных систем и сетей Специалист по взаимодействию с персоналом и пользователями центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Специалист по обнаружению компьютерных атак и инцидентов центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Пути достижения квалификации

Образование и обучение	Среднее профессиональное образование – программы подготовки специалистов среднего звена
Опыт практической работы	-

Особые условия допуска к работе	Наличие допуска к государственной тайне[4] (при необходимости)
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности не реже одного раза в три года

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	3513	Специалисты-техники по компьютерным сетям и системам
ЕКС[5]	-	Техник по защите информации
ОКПДТР[6]	203939	Техник по безопасности компьютерных систем и сетей
Перечни СПО[7]	10.02.05	Обеспечение информационной безопасности автоматизированных систем
	10.02.04	Обеспечение информационной безопасности телекоммуникационных систем

3.1.1. Трудовая функция

Наименование	Установка, настройка и техническое обслуживание средств защиты информации значимых объектов критической информационной инфраструктуры	Код	A/01.5	Уровень (подуровень) квалификации	5

Трудовые действия	Установка средств защиты информации значимых объектов критической информационной инфраструктуры
	Настройка средств защиты информации значимых объектов критической информационной инфраструктуры
	Техническое обслуживание средств защиты информации значимых объектов критической информационной инфраструктуры
Необходимые умения	Проводить установку и монтаж систем средств защиты информации, в том числе СКЗИ, согласно инструкциям по эксплуатации и эксплуатационно-техническим документам
	Проводить настройку средств защиты информации, в том числе СКЗИ, согласно инструкциям по эксплуатации и эксплуатационно-техническим документам
	Проводить техническое обслуживание систем и средств защиты информации согласно инструкциям по эксплуатации и эксплуатационно-технической документации
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Руководящие и методические документы в области защиты информации
	Возможности и назначение допускаемых к эксплуатации на объектах критической информационной инфраструктуры программных, программно-аппаратных (технических) средств обеспечения информационной безопасности: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Принципы построения информационных (автоматизированных) систем и информационно-телекоммуникационных сетей
	Основные информационные технологии, используемые в информационных (автоматизированных) системах и информационно-телекоммуникационных сетях
	Порядок применения средств защиты информации при создании и эксплуатации систем безопасности значимых объектов критической информационной инфраструктуры
	Порядок установки и настройки используемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры средств защиты информации: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Технические описания и инструкции (руководства) по эксплуатации систем и средств защиты информации
	Порядок организации технического обслуживания систем и средств защиты информации согласно инструкциям по эксплуатации и эксплуатационно-технической документации
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Обеспечение работоспособности средств защиты информации значимых объектов критической информационной инфраструктуры	Код	A/02.5	Уровень (подуровень) квалификации	5

Трудовые действия	Контроль работоспособности средств защиты значимых объектов критической информационной инфраструктуры
	Устранение неисправностей и организация ремонта технических (программно-технических) средств защиты информации значимых объектов критической информационной инфраструктуры
	Установка обновлений программного обеспечения средств защиты информации значимых объектов критической информационной инфраструктуры
Необходимые умения	Определять факт нарушения работоспособности средств защиты информации значимых объектов критической информационной инфраструктуры
	Обнаруживать и устранять неисправности средств защиты информации значимых объектов критической информационной инфраструктуры согласно эксплуатационной документации
	Устанавливать обновления программного обеспечения средств защиты информации значимых объектов критической информационной инфраструктуры, не влияющие на непрерывность и надлежащее обеспечение уровня защищенности
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Руководящие и методические документы в области защиты информации
	Назначение и основные характеристики допускаемых к эксплуатации на объектах критической информационной инфраструктуры программных, программно-аппаратных (технических) средств обеспечения информационной безопасности: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Порядок выполнения средствами обеспечения информационной безопасности требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры[8]
	Эксплуатационная и техническая документация на средства защиты информации, применяемые для защиты значимых объектов критической информационной инфраструктуры
	Принципы построения объектов критической информационной инфраструктуры
	Основы построения промышленных сетей передачи данных
Другие характеристики	-

3.1.3. Трудовая функция

Наименование	Регистрация событий и инцидентов информационной безопасности	Код	A/03.5	Уровень (подуровень) квалификации	5

Трудовые действия	Сбор данных для регистрации событий информационной безопасности в значимых объектах критической информационной инфраструктуры
	Прием сообщений об инцидентах от персонала и пользователей (операторов) значимых объектов критической информационной инфраструктуры
	Сбор и регистрация информации об инцидентах информационной безопасности в значимых объектах критической информационной инфраструктуры
	Информирование должностных лиц субъекта критической информационной инфраструктуры об инцидентах информационной безопасности в значимых объектах критической информационной инфраструктуры
	Ведение протоколов и журналов учета при осуществлении мониторинга подсистемы безопасности значимых объектов критической информационной инфраструктуры
Необходимые умения	Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности на значимых объектах критической информационной инфраструктуры
	Формировать отчетность о выявленных событиях и инцидентах информационной безопасности на значимых объектах критической информационной инфраструктуры
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Руководящие и методические документы в области защиты информации
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности
	Основные тактики и техники атак
	Признаки проведения компьютерных атак против находящихся на мониторинге объектов критической информационной инфраструктуры
Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Реализация средствами защиты информации требований обеспечения безопасности значимых объектов критической информационной инфраструктуры	Код	B	Уровень квалификации	6

Возможные наименования должностей, профессий рабочих	Специалист по защите информации в компьютерных системах и сетях Специалист по информационной безопасности

Пути достижения квалификации

Образование и обучение	Высшее образование – бакалавриат или Высшее образование (непрофильное) – бакалавриат и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности
Опыт практической работы	

Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности не реже одного раза в три года[9]

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2523	Специалисты по компьютерным сетям
ЕКС	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Специалист по защите информации
ОКПДТР	203625	Специалист по защите информации в компьютерных системах и сетях
Перечни ВО[10]	10.00.00	Информационная безопасность
	01.00.00	Математика и механика
	02.00.00	Компьютерные и информационные науки
	09.00.00	Информатика и вычислительная техника

3.2.1. Трудовая функция

Наименование	Управление уязвимостями значимых объектов критической информационной инфраструктуры	Код	B/01.6	Уровень (подуровень) квалификации	6

Трудовые действия	Мониторинг уязвимостей и оценка их применимости к значимым объектам критической информационной инфраструктуры
	Определение уровня критичности уязвимостей применительно к значимым объектам критической информационной инфраструктуры
	Определение методов и приоритетов устранения уязвимостей значимых объектов критической информационной инфраструктуры
	Устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей значимых объектов критической информационной инфраструктуры
	Контроль результатов устранения уязвимостей значимых объектов критической информационной инфраструктуры

Необходимые умения	Использовать для мониторинга уязвимостей базы данных, содержащие сведения об известных уязвимостях; официальные информационные ресурсы разработчиков и исследователей программных и программно-аппаратных средств в области информационной безопасности
	Использовать средства анализа защищенности для мониторинга уязвимостей значимых объектов критической информационной инфраструктуры
	Определять уровень опасности уязвимости, ее влияния на информационные системы; проводить расчет критичности уязвимости согласно утвержденным методикам
	Принимать обоснованные решения по выбору метода устранения уязвимости значимого объекта критической информационной инфраструктуры
	Проводить тестирование обновлений программных и программно-аппаратных средств значимых объектов критической информационной инфраструктуры
	Осуществлять разработку и реализацию компенсирующих мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств
	Руководство по организации процесса управления уязвимостями в органе (организации)
	Методика тестирования обновлений программных, программно-аппаратных средств
	Порядок получения и передачи информации в БДУ ФСТЭК России
	Порядок применения компенсирующих мер защиты информации, представленных в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России
	Порядок организации технического обслуживания систем и средств защиты информации согласно инструкциям по эксплуатации и эксплуатационно-технической документации
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Определение порядка, реализация и контроль выполнения средствами защиты информации требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры	Код	B/02.6	Уровень (подуровень) квалификации	6

Трудовые действия	Определение порядка применения средств защиты информации с учетом требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры
	Реализация средствами защиты информации требований, установленных организационно-распорядительными документами по безопасности значимых

	объектов критической информационной инфраструктуры
	Контроль выполнения средствами защиты информации требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры
Необходимые умения	Определять состав и порядок применения средств защиты информации с учетом требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры
	Определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимых объектов критической информационной инфраструктуры
	Контролировать обеспечение средствами защиты информации требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Назначение и основные характеристики допускаемых к эксплуатации на значимых объектах критической информационной инфраструктуры программных, программно-аппаратных (технических) средств обеспечения информационной безопасности: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Порядок реализации средствами обеспечения информационной безопасности требований, установленных организационно-распорядительными документами по безопасности значимых объектов критической информационной инфраструктуры
	Основные меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Основные угрозы безопасности информации и модели нарушителя значимых объектов критической информационной инфраструктуры
	Принципы построения программно-аппаратных комплексов значимых объектов критической информационной инфраструктуры
	Основы построения промышленных сетей передачи данных
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Администрирование средств (управление средствами) защиты информации значимых объектов критической информационной инфраструктуры	Код	B/03.6	Уровень (подуровень) квалификации	6

Трудовые действия	Установка обновлений программного обеспечения средств защиты информации значимых объектов критической информационной инфраструктуры с учетом обеспечения непрерывности и надлежащего уровня защищенности
	Конфигурирование средств защиты информации, используемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры
	Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования значимых объектов критической информационной инфраструктуры
	Проведение занятий с персоналом по работе с системой защиты информации значимых объектов критической информационной инфраструктуры, включая проведение практических занятий с персоналом на киберполигонах или в тестовой зоне
Необходимые умения	Контролировать безотказное функционирование средств защиты информации значимых объектов критической информационной инфраструктуры
	Устанавливать и настраивать общесистемное программное обеспечение с учетом требований по обеспечению защиты информации субъекта критической информационной инфраструктуры
	Настраивать средства защиты информации значимых объектов критической информационной инфраструктуры в том числе средства обеспечения информационной безопасности: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Устанавливать обновления программного обеспечения средств защиты информации значимых объектов критической информационной инфраструктуры
	Обеспечивать бесперебойное функционирование средств защиты информации значимых объектов критической информационной инфраструктуры
Необходимые знания	Принципы формирования политики информационной безопасности субъекта критической информационной инфраструктуры
	Способы и методы администрирования средств обеспечения информационной безопасности: конечных узлов критической информационной инфраструктуры; сетевого уровня, включая средства криптографической защиты; инфраструктуры; пользователей; прикладных программ; данных
	Основы построения корпоративных и промышленных сетей передачи данных
	Технологии защиты от несанкционированного доступа и воздействия вредоносного программного обеспечения информации значимых объектов критической информационной инфраструктуры
	Скриптовые языки, используемые при администрировании средств защиты информации
	Основные криптографические методы, алгоритмы, протоколы, используемые

	для обеспечения безопасности информации
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Обнаружение компьютерных атак и реагирование на инциденты на значимых объектах критической информационной инфраструктуры	Код	C	Уровень квалификации	6

Возможные наименования должностей, профессий рабочих	Инженер информационно-аналитического подразделения Специалист по ликвидации последствий компьютерных инцидентов Специалист по установлению причин компьютерных инцидентов Аналитик центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Пути достижения квалификации

Образование и обучение	Высшее профильное образование – бакалавриат или Высшее образование (непрофильное) – бакалавриат и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности, обнаружения, предупреждения, реагирование на компьютерные инциденты и ликвидации последствий компьютерных атак на информационные ресурсы
Опыт практической работы	Не менее одного года в области информационной безопасности – для сотрудников, имеющих высшее образование (непрофильное)

Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности, обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы не реже одного раза в 3 года

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2529	Специалисты по базам данных и сетям, не входящие в другие группы
ЕКС	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Специалист по защите информации
ОКПДТР	201309	Инженер информационно-аналитического подразделения
Перечни ВО	10.00.00	Информационная безопасность
	01.00.00	Математика и механика
	02.00.00	Компьютерные и информационные науки
	09.00.00	Информатика и вычислительная техника

3.3.1. Трудовая функция

Наименование	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение фактов компьютерных атак	Код	C/01.6	Уровень (подуровень) квалификации	6

Трудовые действия	Получение и использование сведений об актуальных индикаторах компрометации объектов информатизации
	Анализ данных, поступающих от средств мониторинга, с целью выявления инцидентов на мониторируемых значимых объектах критической информационной инфраструктуры
	Сбор информации об инцидентах информационной безопасности, их классификация и оценка потенциала влияния в субъекте критической информационной инфраструктуры
	Обеспечение функционирования механизмов и инициативного информирования работников субъекта критической информационной инфраструктуры о событиях информационной безопасности
Необходимые умения	Анализировать и применять действующую нормативную правовую и методологическую базу, а также положения законодательства Российской Федерации, международные и национальные стандарты в сфере информационной безопасности при мониторинге значимых объектов критической информационной инфраструктуры
	Настраивать средства (агентов, интерфейсов) сбора технических данных для выявления событий информационной безопасности в значимых объектах критической информационной инфраструктуры, в том числе разрабатывать правила корреляции SIEM-систем, а также правила обнаружения атак для IDS/IPS
	Автоматизировать анализ журналов событий информационной безопасности и выявления инцидентов с помощью скриптовых языков
	Определять факт возникновения инцидента информационной безопасности, в том числе компьютерной атаки на значимом объекте критической информационной инфраструктуры
Необходимые знания	Нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Основные уязвимости и информационные угрозы, характерные для значимых объектов критической информационной инфраструктуры
	Порядок настройки средств сбора технических данных для выявления событий информационной безопасности значимых объектов критической информационной инфраструктуры
	Основные тактики и техники атак
	Типичные сетевые атаки на инфраструктуру на различных уровнях модели OSI
	Условия применения технологий доверенного искусственного интеллекта
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Реагирование на инциденты информационной безопасности	Код	C/02.6	Уровень (подуровень) квалификации	6

Трудовые действия	Выполнение действий по реагированию на инциденты информационной безопасности согласно правилам и процедурам реагирования на такие инциденты в субъекте критической информационной инфраструктуры
	Сбор и фиксация артефактов, имеющих отношение к выявленному инциденту информационной безопасности на значимом объекте критической информационной инфраструктуры
	Восстановление в пределах должностных обязанностей функциональных процессов в субъекте критической информационной инфраструктуры с учетом требований по сбору и фиксации данных, имеющих отношение к инцидентам информационной безопасности
	Осуществление взаимодействия в рамках реагирования на инциденты информационной безопасности в субъекте критической информационной инфраструктуры сферы
Необходимые умения	Выполнять реверс-инжиниринг и анализ вредоносного кода
	Выполнять отладку и реверс-инжиниринг приложений архитектуры x86 и ARM, расширять функциональность отладчика и дизассемблера скриптами собственной разработки
	Работать с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности в субъекте критической информационной инфраструктуры
	Применять меры, направленные на снижение тяжести последствий от реализации инцидентов информационной безопасности в субъекте критической информационной инфраструктуры
Необходимые знания	Законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации и обеспечения безопасности критической информационной инфраструктуры
	Уязвимости и информационные угрозы, характерные для значимых объектов критической информационной инфраструктуры
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности
	Язык Assembler для различных архитектур центрального процессора (x86-64, MIPS, ARM, PowerPC)
	Подходы к настройке средств сбора технических данных для выявления событий информационной безопасности
	Принципы работы с техническими средствами, реализующими функции управления инцидентами информационной безопасности
	Подходы к описанию сценариев реализации угроз информационной безопасности в субъектах критической информационной инфраструктуры
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Апостериорный анализ инцидентов информационной безопасности	Код	C/03.6	Уровень (подуровень) квалификации	6

Трудовые действия	Анализ артефактов, имеющих отношение к выявленному инциденту информационной безопасности на значимом объекте критической информационной инфраструктуры

	Описание индикаторов компрометации, связанных с анализируемым инцидентом информационной безопасности
	Анализ и описание уязвимостей объекта критической информационной инфраструктуры, использованных при проведении против него компьютерной атаки
	Подготовка и оформление согласно установленным требованиям материалов в отношении инцидента информационной безопасности для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Необходимые умения	Осуществлять работу с техническими средствами защиты информации, реализующими функции управления инцидентами информационной безопасности
	Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности
	Анализировать вредоносное программное обеспечение, получать индикаторы компрометации
	Оформлять согласно установленным требованиям материалы в отношении инцидента информационной безопасности для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Необходимые знания	Основные уязвимости и информационные угрозы, характерные для субъектов критической информационной инфраструктуры
	Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий информационной безопасности
	Принципы построения систем обеспечения защиты информации и операционной надежности
	Типичные события и инциденты информационной безопасности
	Принципы работы с техническими средствами, реализующими функции управления инцидентами информационной безопасности
	Подходы к описанию сценариев реализации угроз информационной безопасности в субъекте критической информационной инфраструктуры
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Разработка подсистемы безопасности значимых объектов критической информационной инфраструктуры	Код	D	Уровень квалификации	7

Возможные наименования должностей, профессий рабочих	Ведущий специалист по защите информации Главный специалист по защите информации Руководитель проектов в области разработки систем защиты информации Начальник отдела (лаборатории, сектора) защиты информации Руководитель структурного подразделения по обеспечению безопасности значимых объектов критической информационной инфраструктуры

Пути достижения квалификации

Образование и обучение	Высшее образование или Высшее образование (непрофильное) и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности
Опыт практической работы	Не менее трех лет в сфере информационной безопасности

Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности не реже одного раза в три года

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	1330	Руководители служб и подразделений в сфере информационно-коммуникационных технологий
ЕКС	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Специалист по защите информации
ОКПДТР	200593	Главный специалист по защите информации
Перечни ВО	10.05.01	Компьютерная безопасность
	10.05.02	Информационная безопасность телекоммуникационных систем
	10.05.03	Информационная безопасность автоматизированных систем
	10.05.04	Информационно-аналитические системы безопасности
	10.05.05	Безопасность информационных технологий в правоохранительной сфере
	10.05.06[11]	Криптография
	10.05.07[11]	Противодействие техническим разведкам
	10.04.01	Информационная безопасность

3.4.1. Трудовая функция

Наименование	Категорирование объектов критической информационной инфраструктуры	Код	D/01.7	Уровень (подуровень) квалификации	7

Трудовые действия	Инвентаризация, определение состава и ведение локального реестра объектов критической информационной инфраструктуры
	Присвоение объектам критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости
	Подготовка документов, связанных с категорированием объектов критической информационной инфраструктуры
	Реализация взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры

Необходимые умения	Анализировать информационную инфраструктуру субъекта критической информационной инфраструктуры
	Анализировать цели создания и назначение объектов информационной инфраструктуры и решаемые ими задачи, определять объекты информационной инфраструктуры, являющиеся критическими, определять возможные последствия, связанные с негативным воздействием на указанные объекты
	Формировать перечень объектов критической информационной инфраструктуры, подлежащих категорированию
	Готовить документы, связанные с категорированием объектов критической информационной инфраструктуры
	Применять действующие нормативные правовые акты в области обеспечения безопасности информации
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Основные методические и руководящие документы по защите информации в значимых объектах критической информационной инфраструктуры
	Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)
	Методические документы, регламентирующие порядок категорирования объектов критической информационной инфраструктуры
	Основные меры и средства защиты информации значимых объектов критической информационной инфраструктуры
	Последовательность действий при оценке безопасности значимых объектов критической информационной инфраструктуры
	Технические средства контроля эффективности мер защиты информации
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Разработка требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Код	D/02.7	Уровень (подуровень) квалификации	7

Трудовые действия	Анализ характера информации, циркулирующей в информационных системах субъекта критической информационной инфраструктуры, и определение перечня информации, подлежащей защите

	Выявление степени участия персонала в обработке защищаемой информации
	Анализ моделей угроз и нарушителя значимых объектов критической информационной инфраструктуры, сценариев реализации угроз
	Разработка требований по обеспечению информационной безопасности значимых объектов критической информационной инфраструктуры
Необходимые умения	Анализировать цели создания значимых объектов критической информационной инфраструктуры и решаемые ими задачи, анализировать информационную инфраструктуру, определять элементы информационной инфраструктуры, являющиеся критическими, описывать систему взаимодействий между ними
	Анализировать информационную инфраструктуру субъекта критической информационной инфраструктуры
	Выявлять, оценивать и классифицировать угрозы безопасности информации значимых объектов критической информационной инфраструктуры
	Оценивать возможности эксплуатации уязвимостей значимых объектов критической информационной инфраструктуры
	Применять действующие нормативные правовые акты в области обеспечения безопасности информации
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Основные методические и руководящие документы по защите информации в значимых объектах критической информационной инфраструктуры
	Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)
	Локальные нормативные акты, определяющие политику и правила обеспечения информационной безопасности субъекта критической информационной инфраструктуры
	Принципы построения и функционирования систем и сетей передачи информации
	Эталонная модель взаимодействия открытых систем
	Основные меры и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры
	Технические средства контроля эффективности мер защиты информации
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Проектирование и реализация подсистемы безопасности значимых объектов критической информационной инфраструктуры	Код	D/03.7	Уровень (подуровень) квалификации	7

Трудовые действия	Формирование разделов технических заданий на создание подсистем безопасности значимых объектов критической информационной инфраструктуры
	Разработка проектной документации на подсистемы безопасности значимых объектов критической информационной инфраструктуры
	Оформление заявки на разработку подсистемы безопасности значимых объектов критической информационной инфраструктуры
	Проведение технико-экономической оценки проекта подсистемы безопасности значимых объектов критической информационной инфраструктуры
Необходимые умения	Определять комплекс мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры
	Осуществлять выбор средств защиты информации с учетом категории значимости значимого объекта критической информационной инфраструктуры, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию
	Определять политики разграничения доступа (дискреционная, мандатная, ролевая, комбинированная)
	Обосновывать организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимых объектов критической информационной инфраструктуры
	Разрабатывать архитектуру подсистемы безопасности значимых объектов критической информационной инфраструктуры, включающую состав, места установки, взаимосвязи средств защиты информации
Необходимые знания	Методы и технологии проектирования, моделирования, исследования систем защиты значимых объектов критической информационной инфраструктуры
	Этапы создания подсистемы безопасности значимых объектов критической информационной инфраструктуры
	Методы и способы обеспечения безопасности значимых объектов критической информационной инфраструктуры
	Методы и средства, применяемые для обеспечения безопасности критической информационной инфраструктуры, построенные с использованием современных информационных технологий
	Требования к обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Технические средства, технологии и способы обеспечения безопасности значимых объектов критической информационной инфраструктуры
	Порядок проведения процедур закупки высокотехнологичного оборудования, работ, услуг для обеспечения нужд в сфере информационной безопасности
	Технические средства контроля эффективности мер защиты информации
	Регламент учета выявленных инцидентов
	Содержание и порядок деятельности персонала по эксплуатации значимых объектов критической информационной инфраструктуры
	Условия применения технологий доверенного искусственного интеллекта
Другие характеристики	-

3.4.4. Трудовая функция

Наименование	Аудит информационной безопасности значимых объектов критической информационной инфраструктуры	Код	D/04.7	Уровень (подуровень) квалификации	7

Трудовые действия	Разработка программы и методик проведения аудита информационной безопасности значимых объектов критической информационной инфраструктуры
	Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации средств защиты информации значимых объектов критической информационной инфраструктуры
	Проверка состояния организации работ и выполнения организационных и технических требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Оформление материалов аудита информационной безопасности значимых объектов критической информационной инфраструктуры
Необходимые умения	Выполнять экспертизу технической документации значимых объектов критической информационной инфраструктуры
	Разрабатывать программы и методики проведения аудита информационной безопасности значимых объектов критической информационной инфраструктуры
	Использовать экспертно-документальный метод при проведении аудита информационной безопасности значимых объектов критической информационной инфраструктуры
	Проводить анализ ситуаций в области обеспечения безопасности критической информационной инфраструктуры с учетом возможностей, сил и средств проведения компьютерных атак
	Проверять состояние организации работ и выполнения организационных и технических требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Оформлять материалы аудита информационной безопасности значимых объектов критической информационной инфраструктуры
Необходимые знания	Законодательство Российской Федерации, методические документы, национальные стандарты в области информационной безопасности, в области защиты информации и аудита информационной безопасности значимых объектов критической инфраструктуры
	Полномочия органов исполнительной власти, осуществляющих государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и порядок реализации такого контроля
	Методики проведения оценки соответствия уровня информационной безопасности значимых объектов критической информационной инфраструктуры заданным требованиям
	Особенности построения значимых объектов критической информационной инфраструктуры
	Структуры данных служебных полей операционных систем, баз данных и программного обеспечения общего назначения
Другие характеристики	-

3.5. Обобщенная трудовая функция

Наименование	Контроль обнаружения компьютерных атак и реагирования на инциденты на значимых объектах критической информационной инфраструктуры	Код	E	Уровень квалификации	7

Возможные наименования должностей, профессий рабочих	Ведущий специалист по защите информации Руководитель группы подразделения по комплексной защите информации Начальник направления центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Заместитель руководителя центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Руководитель центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Пути достижения квалификации

Образование и обучение	Высшее профильное образование – специалитет, магистратура или Высшее образование (непрофильное) – специалитет, магистратура и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности, обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы
Опыт практической работы	Не менее 3 лет в области информационной безопасности

Особые условия допуска к работе	Наличие допуска к государственной тайне (при необходимости)
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности, обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы не реже одного раза в три года

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	1330	Руководители служб и подразделений в сфере информационно-телекоммуникационных технологий
ЕКС	-	Администратор по обеспечению безопасности информации
	-	Инженер по защите информации
	-	Специалист по защите информации
ОКПДТР	203340	Руководитель группы подразделения по комплексной защите информации

Перечни ВО	10.05.01	Компьютерная безопасность
	10.05.02	Информационная безопасность телекоммуникационных систем
	10.05.03	Информационная безопасность автоматизированных систем
	10.05.04	Информационно-аналитические системы безопасности
	10.05.05	Безопасность информационных технологий в правоохранительной сфере
	10.05.06	Криптография
	10.05.07	Противодействие техническим разведкам
	10.04.01	Информационная безопасность
	01.00.00	Математика и механика
	02.00.00	Компьютерные и информационные науки
	09.00.00	Информатика и вычислительная техника

3.5.1. Трудовая функция

Наименование	Контроль анализа и обработки компьютерных инцидентов на значимых объектах критической информационной инфраструктуры	Код	E/01.7	Уровень (подуровень) квалификации	7

Трудовые действия	Разработка сценариев обнаружения инцидентов информационной безопасности при обработке данных, поступающих с технических средств мониторинга
	Разработка единых правил и процедур реагирования на сообщения о компьютерных инцидентах и атаках, осуществляемых в отношении значимых объектов критической информационной инфраструктуры
	Руководство выявлением событий информационной безопасности и компьютерных атак на мониторируемом значимом объекте критической информационной инфраструктуры
	Информирование федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о статусе и предпринятых действиях по обработке инцидента информационной безопасности в субъекте критической информационной инфраструктуры
Необходимые умения	Применять методологию оценки потенциала влияния (критичности) инцидента информационной безопасности субъекта критической информационной инфраструктуры
	Разрабатывать единые правила и процедуры реагирования на сообщения о компьютерных инцидентах и атаках, осуществляемых в отношении значимых объектов критической информационной инфраструктуры
	Руководить выявлением событий информационной безопасности и компьютерных атак
	Оценивать события информационной безопасности для поиска признаков компьютерных атак
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры

	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Принципы компьютерной и сетевой безопасности в области векторов атак и защиты от них
	Принципы реализации основных технологий обеспечения информационной безопасности
	Технические возможности средств осуществления компьютерных атак и способы их осуществления
	Принципы построения и функционирования систем и сетей передачи информации
	Эталонная модель взаимодействия открытых систем
	Основные угрозы безопасности информации и модели нарушителя значимых объектов критической информационной инфраструктуры
	Основные меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Особенности обеспечения безопасности значимых объектов критической информационной инфраструктуры в конкретной сфере деятельности
	Технические средства контроля эффективности мер защиты информации
	Условия применения технологий доверенного искусственного интеллекта
Другие характеристики	-

3.5.2. Трудовая функция

Наименование	Организация расследования компьютерных инцидентов на значимых объектах критической информационной инфраструктуры	Код	E/02.7	Уровень (подуровень) квалификации	7

Трудовые действия	Разработка единых правил и процедур реагирования на инциденты информационной безопасности, выявленные на значимом объекте критической информационной инфраструктуры
	Руководство расследованием компьютерных инцидентов на значимом объекте критической информационной инфраструктуры
	Определение критериев для оценки условий закрытия инцидента информационной безопасности в субъекте критической информационной инфраструктуры
	Осуществление взаимодействия в рамках проведения расследования и восстановления после инцидентов информационной безопасности в субъекте критической информационной инфраструктуры, в том числе с внешними заинтересованными организациями
Необходимые умения	Разрабатывать правила и процедуры реагирования на инциденты информационной безопасности в субъекте критической информационной инфраструктуры
	Принимать управленческие решения при реагировании на компьютерные инциденты
	Оценивать последствия выявленных инцидентов
	Организовывать взаимодействие при расследовании инцидентов

	информационной безопасности
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Модель угроз информационной безопасности, модель нарушителя информационной безопасности субъекта
	Критерии несанкционированного воздействия на значимые объекты критической информационной инфраструктуры
	Критерии оценки защищенности значимых объектов критической информационной инфраструктуры
	Технические средства контроля эффективности мер защиты информации
	Регламент информирования персонала значимых объектов критической информационной инфраструктуры о выявленных инцидентах
	Регламент учета выявленных инцидентов
	Регламент устранения инцидентов
	Содержание и порядок деятельности персонала по эксплуатации значимых объектов критической информационной инфраструктуры и систем безопасности значимых объектов критической информационной инфраструктуры
Другие характеристики	-

3.5.3. Трудовая функция

Наименование	Контроль апостериорного анализа компьютерных инцидентов	Код	E/03.7	Уровень (подуровень) квалификации	7

Трудовые действия	Анализ выявленных инцидентов на значимых объектах критической информационной инфраструктуры
	Проверка работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик в субъектах критической информационной инфраструктуры
	Оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик в субъектах критической информационной инфраструктуры
	Определение уровня защищенности значимых объектов критической информационной инфраструктуры в субъектах критической информационной инфраструктуры
Необходимые умения	Определять параметры функционирования программно-аппаратных средств защиты информации в субъекте критической информационной инфраструктуры

	Разрабатывать методики оценки защищенности значимых объектов критической информационной инфраструктуры в субъектах критической информационной инфраструктуры
	Оценивать эффективность защиты информации в субъектах критической информационной инфраструктуры
	Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации значимых объектов критической информационной инфраструктуры
	Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности значимых объектов критической информационной инфраструктуры, в том числе с применением инструментов (методик) автоматизированного поиска уязвимостей
	Применять методики анализа защищенности операционных систем
Необходимые знания	Нормативные правовые акты, методические документы, национальные стандарты в области информационной безопасности, защиты информации и аудита информационной безопасности значимых объектов критической информационной инфраструктуры
	Методы и методики оценки безопасности программно-аппаратных средств защиты информации
	Принципы построения программно-аппаратных средств защиты информации значимых объектов критической информационной инфраструктуры
	Принципы построения подсистем безопасности значимых объектов критической информационной инфраструктуры
	Структура и принципы работы исполняемых файлов в операционных системах Windows и Linux
	Способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности субъекта критической информационной инфраструктуры
	Способы выявления уязвимостей, угроз безопасности информации и методы технической защиты информации от них
Другие характеристики	-

3.6. Обобщенная трудовая функция

Наименование	Управление обеспечением безопасности значимых объектов критической информационной инфраструктуры	Код	F	Уровень квалификации	8

Возможные наименования должностей, профессий рабочих	Директор по развитию цифровых технологий документированных сфер деятельности организации Заместитель генерального директора по информационной безопасности

Пути достижения квалификации

Образование и обучение	Высшее профильное образование – специалитет, магистратура или Высшее образование (непрофильное) – специалитет, магистратура и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности

Опыт практической работы	Не менее 3 лет в сфере информационной безопасности, включая не менее 2 лет на руководящих должностях – для сотрудников, имеющих высшее профильное образование Не менее 5 лет в области информационной безопасности, включая не менее 3 лет на руководящих должностях – для сотрудников, имеющих высшее образование (непрофильное)
Особые условия допуска к работе	-
Другие характеристики	Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности не реже одного раза в три года

Справочная информация

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	1213	Руководители в области определения политики и планирования деятельности
ЕКС	-	Главный специалист по технической защите информации
ОКПДТР	200847	Директор по развитию цифровых технологий документированных сфер деятельности организации
	201343	Главный специалист по защите информации
Перечни ВО	10.05.01	Компьютерная безопасность
	10.05.02	Информационная безопасность телекоммуникационных систем
	10.05.03	Информационная безопасность автоматизированных систем
	10.05.04	Информационно-аналитические системы безопасности
	10.05.05	Безопасность информационных технологий в правоохранительной сфере
	10.05.06	Криптография
	10.05.07	Противодействие техническим разведкам
	10.04.01	Информационная безопасность
ОКСВНК[11]	2.3.6.	Методы и системы защиты информации, информационная безопасность
	1.2.4.	Кибербезопасность

3.6.1. Трудовая функция

Наименование	Определение измеримых и практических результатов деятельности по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Код	F/01.8	Уровень (подуровень) квалификации	8

Трудовые действия	Определение влияния информационных технологий на деятельность субъекта критической информационной инфраструктуры
	Определение основных негативных последствий, наступление которых возможно в результате реализации угроз безопасности информации
	Разработка модели угроз и модели нарушителя безопасности значимых объектов критической информационной инфраструктуры
	Организация категорирования объектов критической информационной инфраструктуры

	Формирование требований по защите информации, обрабатываемой в значимых объектах критической информационной инфраструктуры, включая использование математического аппарата для решения прикладных задач
	Выбор и обоснование критериев эффективности функционирования значимых объектов критической информационной инфраструктуры
Необходимые умения	Анализировать и применять методологическую базу, положения нормативных правовых актов Российской Федерации, международных и национальных стандартов в области обеспечения защиты информации и информационной безопасности значимых объектов КИИ
	Определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры, подлежащих защите
	Классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры с учетом специфики сферы деятельности
	Разрабатывать модели угроз безопасности информации и нарушителей значимых объектов критической информационной инфраструктуры
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Функции органов исполнительной власти, осуществляющих государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и порядок реализации такого контроля
	Нормативные правовые акты, регулирующие уголовную ответственность за деяния, связанные с нарушением безопасности значимых объектов критической информационной инфраструктуры
	Нормативные правовые акты, регулирующие административную ответственность за правонарушения, связанные с нарушением обеспечения безопасности объектов критической информационной инфраструктуры
	Руководящие и методические документы: в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации; в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; в области выработки и реализации государственной политики, нормативно-правового регулирования в области связи
	Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)

	Локальные нормативные акты, определяющие политику и правила обеспечения информационной безопасности субъекта критической информационной инфраструктуры
	Методика моделирования угроз информационной безопасности
	Основные угрозы безопасности информации для значимых объектов критической информационной инфраструктуры
	Основные меры по защите информации в значимых объектах критической информационной инфраструктуры
	Особенности защиты информации в значимых объектах критической информационной инфраструктуры с учетом специфики сферы деятельности
	Технические средства контроля эффективности мер защиты информации
Другие характеристики	-

3.6.2. Трудовая функция

Наименование	Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Код	F/02.8	Уровень (подуровень) квалификации	8

Трудовые действия	Организация разработки политики информационной безопасности субъекта критической информационной инфраструктуры
	Организация работ по разработке моделей угроз и нарушителей безопасности информации для значимых объектов критической информационной инфраструктуры
	Организация работы комиссии по категорированию объектов критической информационной инфраструктуры
	Подготовка (разработка) документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации
	Проведение (разработка) проверки полноты описания в организационно-распорядительных документах действий персонала по реализации организационных мер защиты информации
Необходимые умения	Разрабатывать проекты внутренних документов (локальные акты, организационно-распорядительные документы и методические материалы) субъекта критической информационной инфраструктуры, устанавливающих цели и принципы, а также определяющих методологию и правила управления информационной безопасностью
	Анализировать и обосновывать общую стратегию субъекта критической информационной инфраструктуры по вопросам управления процессами обеспечения информационной безопасности согласно законодательству Российской Федерации на основе современных методов и лучших практик
	Реализовывать политику в области обеспечения информационной безопасности по вопросам управления процессами обеспечения информационной безопасности и операционной надежности
	Устанавливать требования к процессу мониторинга состояния безопасности значимых объектов критической информационной инфраструктуры
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры

	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Функции органов исполнительной власти, осуществляющих государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и порядок реализации такого контроля
	Нормативные правовые акты, регулирующие уголовную ответственность за деяния, связанные с нарушением безопасности значимых объектов критической информационной инфраструктуры
	Нормативные правовые акты, регулирующие административную ответственность за правонарушения, связанные с нарушением обеспечения безопасности объектов критической информационной инфраструктуры
	Руководящие и методические документы: в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации; в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; в области выработки и реализации государственной политики, нормативно-правового регулирования в области связи
	Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)
	Локальные нормативные акты, определяющие политику и правила обеспечения информационной безопасности в субъекте критической информационной инфраструктуры
	Содержание и порядок деятельности персонала по эксплуатации подсистем безопасности значимых объектов критической информационной инфраструктуры
	Основные угрозы безопасности информации значимых объектов критической информационной инфраструктуры
Другие характеристики	-

3.6.3. Трудовая функция

Наименование	Организация мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Код	F/03.8	Уровень (подуровень) квалификации	8

Трудовые действия	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры

	Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Организация мероприятий по мониторингу состояния защищенности значимых объектов критической информационной инфраструктуры и реагированию на компьютерные инциденты
	Организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности
	Организация формирования и развития навыков работников организации в сфере информационной безопасности
Необходимые умения	Анализировать и обосновывать общую стратегию субъекта критической информационной инфраструктуры по вопросам обеспечения защиты информации и операционной надежности согласно законодательству Российской Федерации на основе современных методов и лучших практик
	Оценивать эффективность деятельности по выполнению работ, связанных с обеспечением защиты информации и операционной надежности
	Организовывать и осуществлять деятельность по проверке готовности субъекта критической информационной инфраструктуры противостоять угрозам информационной безопасности
	Совершенствовать систему безопасности значимых объектов критической информационной инфраструктуры
	Осуществлять взаимодействие с федеральными органами исполнительной власти от лица субъекта критической информационной инфраструктуры по вопросам безопасности значимых объектов критической информационной инфраструктуры
Необходимые знания	Основные понятия, используемые в нормативных правовых актах, регламентирующих вопросы защиты критической информационной инфраструктуры
	Принципы обеспечения безопасности критической информационной инфраструктуры
	Нормативные правовые основы по обеспечению безопасности значимых объектов критической информационной инфраструктуры
	Положения правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры
	Механизм организации и координации деятельности государственных органов по защите критической информационной инфраструктуры
	Права и обязанности субъектов критической информационной инфраструктуры, иных органов и организаций при защите критической информационной инфраструктуры, а также в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
	Функции органов исполнительной власти, осуществляющих государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и порядок реализации такого контроля
	Нормативные правовые акты, регулирующие уголовную ответственность за деяния, связанные с нарушением безопасности значимых объектов критической информационной инфраструктуры
	Нормативные правовые акты, регулирующие административную ответственность за правонарушения, связанные с нарушением обеспечения безопасности объектов критической информационной инфраструктуры
	Порядок проведения процедур закупки высокотехнологичного оборудования, работ, услуг для обеспечения нужд в сфере информационной безопасности

	Ключевые показатели эффективности деятельности субъекта критической информационной инфраструктуры по обеспечению защиты информации и операционной надежности
	Принципы целеполагания, виды и методы организационного планирования
	Принципы построения архитектуры подсистемы безопасности значимых объектов критической информационной инфраструктуры
	Состав и содержание, а также порядок применения организационных и технических мер обеспечения защиты информации и операционной надежности субъектов критической информационной инфраструктуры
	Нормы профессиональной этики
	Условия применения доверенных технологий искусственного интеллекта
Другие характеристики	-

IV. Сведения об организациях – разработчиках профессионального стандарта

4.1. Ответственная организация-разработчик

Ассоциация защиты информации, город Москва	
Президент	Лось Владимир Павлович

4.2. Наименования организаций-разработчиков

1	ФГАОУ ВО «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И. М. Губкина», город Москва
2	ФГАОУ ДПО «Институт повышения квалификации руководящих работников и специалистов топливно-энергетического комплекса», город Москва
3	АНО ДПО центр повышения квалификации «АИС», город Москва
4	ФГБУ «ВНИИ труда» Минтруда России, город Москва
5	ФУМО в системе ВО по УГСНП «Информационная безопасность», город Москва
6	Ассоциация предприятий компьютерных и информационных технологий, город Москва
7	ФГКОУ ВО «Академия Федеральной службы безопасности Российской Федерации», город Москва
8	ФУМО в системе СПО по УГПС «Информационная безопасность», город Москва

V. Сокращения, используемые в профессиональном стандарте

x86 – семейство микропроцессорных архитектур с обратной совместимостью инструкций, разработанное компанией Intel
СКЗИ – средства криптографической защиты информации
БДУ - банк данных угроз безопасности информации
ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации

---

[1] Общероссийский классификатор занятий.
[2] Приказ Минтруда России от 29 сентября 2014 г. № 667н «О реестре профессиональных стандартов (перечне видов профессиональной деятельности)» (зарегистрирован Минюстом России 19 ноября 2014 г., регистрационный № 34779) с изменением, внесенным приказом Минтруда России от 9 марта 2017 г. № 254н (зарегистрирован Минюстом России 29 марта 2017 г., регистрационный № 46168).
[3] Общероссийский классификатор видов экономической деятельности.
[4] Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

[5] Единый квалификационный справочник должностей руководителей, специалистов и служащих.

[6] Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов.

[7] Приказ Минпросвещения России от 17 мая 2022 г. № 336 «Об утверждении перечней профессий и специальностей среднего профессионального образования и установлении соответствия отдельных профессий и специальностей среднего профессионального образования, указанных в этих перечнях, профессиям и специальностям среднего профессионального образования, перечни которых утверждены приказом Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 «Об утверждении перечней профессий и специальностей среднего профессионального образования» (зарегистрирован Минюстом России 17 июня 2022 г., регистрационный № 68887) с изменениями, внесенными приказами Минпросвещения России от 12 мая 2023 г. № 359 (зарегистрирован Минюстом России 9 июня 2023 г., регистрационный № 73797), от 25 сентября 2023 г. № 717 (зарегистрирован Минюстом России 26 октября 2023 г., регистрационный № 75754), от 27 апреля 2024 г. № 289 (зарегистрирован Минюстом России 31 мая 2024 г., регистрационный № 78367), от 7 ноября 2024 г. № 782 (зарегистрирован Минюстом России 10 декабря 2024 г., регистрационный № 80517), от 25 марта 2025 г. № 226 (зарегистрирован Минюстом России 29 апреля 2025 г., регистрационный № 82008), от 16 сентября 2025 г. № 667 (зарегистрирован Минюстом России 16 октября 2025 г., регистрационный № 83852), от 19 февраля 2026 г. № 106 (зарегистрирован Минюстом России 26 марта 2026 г., регистрационный № 85749).

[8] Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован Минюстом России 26 марта 2018 г., регистрационный № 50524) с изменениями, внесенными приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071), приказом ФСТЭК России от 26 марта 2019 г. № 60 (зарегистрирован Минюстом России 18 апреля 2019 г., регистрационный № 54443), приказом ФСТЭК России от 20 февраля 2020 г. № 35 (зарегистрирован в Минюстом России 11 сентября 2020 г., регистрационный № 59793), приказом ФСТЭК России от 28 августа 2024 г. № 159 (зарегистрирован Минюстом России 24 октября 2024 г., регистрационный № 79900).

[9] Приказ ФСТЭК от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный № 50118) с изменениями, внесенными приказами ФСТЭК от 27 марта 2019 г. № 64 (зарегистрирован Минюстом России 13 июня 2019 г., регистрационный № 54920), от 20 апреля 2023 г. № 69 (зарегистрирован Минюстом 23 июня 2023 г., регистрационный № 73969).

[10] Приказ Минобрнауки России от 12 сентября 2013 г. № 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования» (зарегистрирован Минюстом России 14 октября 2013 г., регистрационный № 30163) с изменениями, внесенными приказами Минобрнауки России от 29 января 2014 г. № 63 (зарегистрирован Минюстом России 28 февраля 2014 г., регистрационный № 31448), от 20 августа 2014 г. № 1033 (зарегистрирован Минюстом России 3 сентября 2014 г., регистрационный № 33947), от 13 октября 2014 г. № 1313 (зарегистрирован Минюстом России 13 ноября 2014 г., регистрационный № 34691), от 25 марта 2015 г. № 270 (зарегистрирован Минюстом России 22 апреля 2015 г., регистрационный № 36994), от 1 октября 2015 г. № 1080 (зарегистрирован Минюстом России 19 октября 2015 г., регистрационный № 39355), от 1 декабря 2016 г. № 1508 (зарегистрирован Минюстом России 20 декабря 2016 г., регистрационный № 44807), от 10 апреля 2017 г. № 320 (зарегистрирован Минюстом России 10 мая 2017 г., регистрационный № 46662), от 11 апреля 2017 г. № 328 (зарегистрирован Минюстом России 23 июня 2017 г., регистрационный № 47167), от 23 марта 2018 г. № 210 (зарегистрирован Минюстом России 11 апреля 2018 г., регистрационный № 50727), от 30 августа 2019 г. № 664 (зарегистрирован Минюстом России 23 сентября 2019 г., регистрационный № 56026), от 15 апреля 2021 г. № 296 (зарегистрирован Минюстом России 27 апреля 2021 г., регистрационный № 63245), от 13 декабря 2021 г. № 1229 (зарегистрирован Минюстом России 13 апреля 2022 г., регистрационный № 68183). В соответствии с абзацем седьмым пункта 2 приказа Минобрнауки России от 1 февраля 2022 г. № 89 (зарегистрирован Минюстом России 3 марта 2022 г., регистрационный № 67610) с изменениями, внесенными приказами Минобрнауки России от 29 августа 2022 г. № 822 (зарегистрирован Минюстом России 15 ноября 2022 г., регистрационный № 70948), от 2 августа 2024 г. № 514 (зарегистрирован Минюстом России 16 августа 2024 г., регистрационный № 79187), от 27 марта 2026 г. № 201 (зарегистрирован Минюстом России 27 апреля 2026 г., регистрационный № 86219), срок действия ограничен до 1 сентября 2027 г.

[11] Перечни специальностей и направлений подготовки высшего образования по программам бакалавриата, программам специалитета, программам магистратуры, с указанием квалификации, присваиваемой по соответствующим специальностям и направлениям подготовки высшего образования, устанавливаемые Министерством науки и высшего образования Российской Федерации в соответствии с частью 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»; подпункт 4.2.1 пункта 4 Положения о Министерстве науки и высшего образования Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 15 июня 2018 г. № 682.

[12] Общероссийский классификатор специальностей высшей научной квалификации.