УТВЕРЖДЕН

приказом Министерства

труда и социальной защиты   
Российской Федерации

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2021\_\_ г. №\_\_\_\_

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

**Специалист по информационной безопасности**

**в кредитно-финансовой сфере**

|  |
| --- |
|  |
| Регистрационный номер |

**I. Общие сведения**

|  |  |  |
| --- | --- | --- |
| Обеспечение информационной безопасности в организациях кредитно-финансовой сферы |  |  |
| (наименование вида профессиональной деятельности) | | Код |

Основная цель вида профессиональной деятельности:

|  |
| --- |
| Управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |

Группа занятий:

|  |  |  |  |
| --- | --- | --- | --- |
| 1330 | Руководители служб и подразделений в сфере информационно-коммуникационных технологий | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| (код ОКЗ[[1]](#endnote-1)) | (наименование) | (код ОКЗ) | (наименование) |

Отнесение к видам экономической деятельности:

|  |  |
| --- | --- |
| 74.90.9 | Деятельность в области защиты информации |
| (код ОКВЭД[[2]](#endnote-2)) | (наименование вида экономической деятельности) |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| код | Наименование | Наименование | код | уровень (подуровень) квалификации |
| А | Организация процессов обеспечения информационной безопасности в организациях кредитно-финансовой сферы | Организация управления рисками информационной безопасности в организациях кредитно-финансовой сферы | A/01.8 | 8 |
| Организация обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | A/02.8 | 8 |
| Совершенствование системы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | A/03.8 | 8 |
| Контроль процессов управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | A/04.8 | 8 |
| B | Аналитическое сопровождение деятельности по управлению рисками информационной безопасности в организациях кредитно-финансовой сферы | Моделирование угроз безопасности информации в организациях кредитно-финансовой сферы | B/01.7 | 7 |
| Выявление, идентификация и оценка риска информационной безопасности в организациях кредитно-финансовой сферы | B/02.7 | 7 |
| Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях кредитно-финансовой сферы | B/03.7 | 7 |
| Разработка мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности в организациях кредитно-финансовой сферы | B/04.7 | 7 |
| Мониторинг риска информационной безопасности и контроль показателей уровня риска информационной безопасности в организациях кредитно-финансовой сферы | B/05.7 | 7 |
| C | Методологическое обеспечение процессов информационной безопасности в организациях кредитно-финансовой сферы | Разработка политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации | C/01.7 | 7 |
| Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | C/02.7 | 7 |
| Разработка методологии управления рисками информационной безопасности в организациях кредитно-финансовой сферы | C/03.7 | 7 |
| Разработка методологии выявления, реагирования и восстановления после инцидентов информационной безопасности в организациях кредитно-финансовой сферы | C/04.7 | 7 |
| D | Обеспечение информационной безопасности в организациях кредитно-финансовой сферы | Реализация процессов защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | D/01.6 | 6 |
| Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | D/02.6 | 6 |
| Реализация программ повышения осведомленности по вопросам противодействия реализации информационных угроз в организациях кредитно-финансовой сферы | D/03.6 | 6 |
| Е | Управление инцидентами информационной безопасности в организациях кредитно-финансовой сферы | Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак | Е/01.6 | 6 |
| Реагирование на инциденты информационной безопасности | Е/02.6 | 6 |
| Восстановление после реализации инцидентов информационной безопасности | Е/03.6 | 6 |

**III. Характеристика обобщенных трудовых функций**

# 3.1. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Организация процессов обеспечения информационной безопасности в организациях кредитно-финансовой сферы | Код | A | Уровень квалификации | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Руководитель структурного подразделения  Руководитель департамента  Руководитель управления |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование – магистратура или специалитет или  Высшее образование (непрофильное) – магистратура или специалитет и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационной безопасности |
| Требования к опыту практической работы | не менее 5 лет в области информационной безопасности, в том числе на руководящих должностях не менее 3 лет |
| Особые условия допуска к работе | - |
| Другие характеристики |  |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 1330 | Руководители служб и подразделений в сфере информационно-коммуникационных технологий |
| ЕКС | - | Начальник отдела (лаборатории, сектора) по технической защите информации |
| ОКПДТР | 46115 | Руководитель аналитической группы подразделения по комплексной защите информации |
| ОКСО[[3]](#endnote-3) | 1.02.04.01 | Математика и компьютерные науки |
| 1.02.04.02 | Фундаментальная информатика и информационные технологии |
| 1.02.04.03 | Математическое обеспечение и администрирование информационных систем |
| 2.09.04.02 | Информационные системы и технологии |
| 2.09.04.03 | Прикладная информатика |
| 2.09.04.04 | Программная инженерия |
| 2.10.04.01 | Информационная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационная безопасность автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |

## 3.1.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Организация управления рисками информационной безопасности в организациях кредитно-финансовой сферы | Код | A/01.8 | Уровень (подуровень) квалификации | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка предложений по содержанию политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации |
| Разработка предложений по мероприятиям (мерам), направленным на уменьшение негативного влияния риска информационной безопасности |
| Планирование работы, установление функций, обязанностей и определение контрольных показателей эффективности для курируемых подразделений в организации кредитно-финансовой сферы |
| Организация процесса обеспечения осведомленности об актуальных информационных угрозах |
| Подготовка информационно-аналитических материалов по вопросам управления рисками информационной безопасности в организациях кредитно-финансовой сферы |
| Организация деятельности по реализации процедур управления риском внутреннего нарушителя в отношении работников в организации кредитно-финансовой сферы |
| Оценка ресурсного (кадрового и финансового) обеспечения для планирования, реализации, контроля и совершенствования процессов системы управления рисками информационной безопасности в организации кредитно-финансовой сферы |
| Организация работы по формированию отчетности в рамках управления рисками информационной безопасности в организации кредитно-финансовой сферы |
| Организация работы по выявлению, регистрации, реагированию и восстановлению после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Оценивать эффективность управления риском информационной безопасности, в том числе оценивать эффективность выявления событий риска информационной безопасности |
| Обосновывать предложения по изменению и совершенствованию процесса управления рисками информационной безопасности |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы, а также определяющих методологию и правила по управлению рисками информационной безопасности в организации кредитно-финансовой сферы |
| Анализировать и обосновывать общую стратегию организации кредитно-финансовой сферы по вопросам управления рисками информационной безопасности в соответствии с законодательством на основе современных методов и лучших практик |
| Реализовывать политику в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации |
| Устанавливать требования к процессу мониторинга риска информационной безопасности и контролю фактических значений уровня риска информационной безопасности |
| Определение правил и требований к реализации процессов выявления, идентификации и оценки рисков информационной безопасности |
| Необходимые знания | Законодательство Российской Федерации, нормативная документация Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы управления подразделениями, задействованными в реализации мер по управлению рисками информационной безопасности в организации кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации в организациях кредитно-финансовой сферы |
| Принципы целеполагания, виды и методы организационного планирования |
| Нормы профессиональной этики |
| Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) организации кредитно-финансовой сферы |
| Подходы к определению показателей эффективности деятельности организации кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.1.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Организация обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | A/02.8 | Уровень (подуровень) квалификации | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Подготовка предложений по определению стратегических целей и задач организации кредитно-финансовой сферы по вопросам обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Подготовка информационно-аналитических материалов по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Организация работы по формированию отчетности по защите информации и обеспечению операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация работы по выявлению, регистрации, реагированию и восстановлению после инцидентов, связанных с реализацией информационных угроз |
| Организация разработки и контроль за реализацией организационных и технических мер по обеспечению защиты информациии и операционной надежности (киберустойчивости) |
| Планирование работы, установление функций, обязанностей и определение контрольных показателей эффективности для курируемых подразделений в организации кредитно-финансовой сферы |
| Разработка проектов внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы, определяющих методологию и правила по обеспечению защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация и осуществление деятельности по сценарному анализу и тестированию готовности кредитно-финансовой сферы противостоять реализации информационных угроз |
| Организация работы по выявлению, приоритизации, классификации и устранению уязвимостей в критичной архитектуре, контролю полноты и своевременности устранения выявленных уязвимостей |
| Оценка ресурсного (кадрового и финансового) обеспечения для планирования, реализации, контроля и совершенствования процессов обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация работы по идентификации критичной архитектуры |
| Организация работ по выполнению процессов защиты информации в кредитно-финансовой сфере |
| Необходимые умения | Анализировать и обосновывать общую стратегию организации кредитно-финансовой сферы по вопросам обеспечения защиты информации и операционной надежности (киберустойчивости) в соответствии с законодательством, на основе современных методов и лучших практик |
| Применять риск-ориентированный подход к выбору объектов информатизации, подвергаемых тестированию на проникновение |
| Оценивать эффективность деятельности по выполнению работ, связанных с обеспечением защиты информации и операционной надежности (киберустойчивости) |
| Устанавливать, применять и контролировать внутренние стандарты конфигурирования объектов информатизации (стандартов конфигурирования) |
| Организовывать и осуществлять деятельность по тестированию готовности организации кредитно-финансовой сферы противостоять реализации информационных угроз |
| Разрабатывать и использовать сценарии, включающие значительные финансовые потери, в рамках проведения стресс-тестирований для определения потенциала влияния и уровня риска для бизнес-модели финансовой организации |
| Необходимые знания | Законодательство Российской Федерации, нормативная документация Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) организации кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы целеполагания, виды и методы организационного планирования |
| Подходы к идентификации критичной архитектуры |
| Состав и содержание, а также порядок применения организационных и технических мер обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Нормы профессиональной этики |
| Другие характеристики |  |

## 3.1.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Совершенствование системы управления рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | A/03.8 | Уровень (подуровень) квалификации | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка предложений по совершенствованию процессов управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Планирование внедрения тактических и стратегических улучшений процессов управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация деятельности по реализации тактических и стратегических улучшений процессов управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Обеспечение участия курируемых подразделений в контроле за деятельностью, связанной с реализацией тактических и стратегических улучшений процессов управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые умения | Устанавливать и поддерживать деловые контакты, связи, отношения с сотрудниками и заинтересованными сторонами по вопросам управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Анализировать и обосновывать общую стратегию организации кредитно-финансовой сферы по вопросам управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Обосновывать предложения по изменению и совершенствованию стратегии управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Определять источники информации для проведения анализа необходимости совершенствования процессов управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы целеполагания, виды и методы организационного планирования |
| Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) организации кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные подходы к проектному управлению |
| Нормы профессиональной этики |
| Другие характеристики |  |

## 3.1.4. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Контроль процессов управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | A/04.8 | Уровень (подуровень) квалификации | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Организация работ по установлению и реализации программ контроля и аудита обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Обеспечение сопровождения проведения оценки эффективности системы управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Организация работы по мониторингу риска информационной безопасности в организации кредитно-финансовой сферы |
| Определение правил и требований к контролю процессов управления риском информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация работы по формированию отчетности в рамках управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые умения | Обосновывать предложения по изменению и совершенствованию процессов обеспечения защиты информации и операционной надежности (киберустойчивости) по результатам реализации программ контроля и аудита обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Обосновывать предложения по изменению и совершенствованию процессов управления риском информационной безопасности по результатам оценки эффективности системы управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Применять требования нормативных правовых актов и методологических документов по управлению рисками информационной безопасности, обеспечению защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Определять подходы к организации мониторинга риска информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы целеполагания, виды и методы организационного планирования |
| Подходы к организации отчетности в рамках управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Ключевые показатели эффективности деятельности по управлению рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) организации кредитно-финансовой сферы |
| Другие характеристики |  |

# 3.2. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Аналитическое сопровождение деятельности по управлению рисками информационной безопасности в организациях кредитно-финансовой сферы | Код | B | Уровень квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Главный специалист по информационной безопасности  Ведущий специалист по информационной безопасности |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование |
| Требования к опыту практической работы | Не менее 3 лет в области информационной безопасности в организации кредитно-финансовой сферы |
| Особые условия допуска к работе | - |
| Другие характеристики |  |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Главный специалист по технической защите информации |
| ОКПДТР | 20911 | Главный специалист по защите информации |
| ОКСО |  |  |
| 2.09.03.02 | Информационные системы и технологии |
| 2.09.03.03 | Прикладная информатика |
| 2.09.03.04 | Программная инженерия |
| 2.10.03.01 | Информационная безопасность |
| 1.02.04.01 | Математика и компьютерные науки |
| 1.02.04.02 | Фундаментальная информатика и информационные технологии |
| 1.02.04.03 | Математическое обеспечение и администрирование информационных систем |
| 2.09.04.02 | Информационные системы и технологии |
| 2.09.04.03 | Прикладная информатика |
| 2.09.04.04 | Программная инженерия |
| 2.10.04.01 | Информационная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационная безопасность автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |

## 3.2.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Моделирование угроз безопасности информации в организациях кредитно-финансовой сферы | Код | B/01.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение и анализ информационных угроз, характерных для организаций кредитно-финансовой сферы |
| Определение возможных сценариев реализации информационных угроз в организации кредитно-финансовой сферы |
| Организация процесса выявления возможных уязвимостей критичной архитектуры |
| Формирование модели внутреннего и внешнего нарушителя безопасности информации в организации кредитно-финансовой сферы |
| Подготовка модели угроз информационной безопасности, направленных на организацию кредитно-финансовой сферы |
| Определение возможных источников информационных угроз (путем анализа каналов реализации таких угроз в отношении критичной архитектуры) |
| Оценка возможности эксплуатации уязвимостей в отношении критичной архитектуры |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Анализировать ландшафт информационных угроз, актуальных для организаций кредитно-финансовой сферы |
| Разрабатывать модели угроз беопасности информации в организации кредитно-финансовой сферы |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы |
| Оценивать потенциал нарушителя безопасности информации |
| Осуществлять сбор и анализ информации об актуальных информационных угрозах и уязвимостях |
| Разрабатывать возможные сценарии реализации информационных угроз в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Основные риски информационной безопасности в рамках бизнес- и технологических процессов организаций кредитно-финансовой сферы |
| Основные информационные угрозы и уязвимости в организациях кредитно-финансовой сферы |
| Основы функционирования объектов информатизации в организации кредитно-финансовой сферы |
| Основы построения вычислительных сетей в организации кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.2.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Выявление, идентификация и оценка риска информационной безопасности в организациях кредитно-финансовой сферы | Код | B/02.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Идентификация риска информационной безопасности в организации кредитно-финансовой сферы |
| Проведение оценки риска информационной безопасности по каждому виду деятельности организации кредитно-финансовой сферы |
| Организация и выполнение оценки степени вероятности возникновения инцидентов информационной безопасности |
| Проведение оценки степени тяжести последствий в результате инцидентов информационной безопасности |
| Проведение анализа базы событий риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация и проведение самооценки (анкетирование) риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация и проведение интервьюирования работников организации кредитно-финансовой сферы в целях идентификации риска информационной безопасности |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Применять методологию для проведения оценки риска информационной безопасности по каждому виду деятельности организации кредитно-финансовой сферы |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы |
| Разрабатывать предложения по совершенствованию внутренних документов организации кредитно-финансовой сферы, определяющих методологию оценки рисков информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основы проведения анализа баз данных |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные риски информационной безопасности в рамках бизнес- и технологических процессов организаций кредитно-финансовой сферы |
| Подходы и лучшие практики по оценке рисков информационной безопасности |
| Классификация событий риска информационной безопасности организаций кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.2.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях кредитно-финансовой сферы | Код | B/03.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Выявление и классификация событий риска информационной безопасности в кредитно-финансовой сфере |
| Ведение базы данных и регистрация событий риска информационной безопасности кредитно-финансовой сферы |
| Определение потерь от реализации событий риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация сбора информации о событиях риска информационной безопасности организации кредитно-финансовой сферы |
| Проведение анализа причин и последствий реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы по ведению базы событий риска информационной безопасности организации кредитно-финансовой сферы |
| Обеспечивать ведение базы данных событий риска информационной безопасности кредитно-финансовой сферы |
| Применять методологию для проведения оценки потерь от реализации риска информационной безопасности в организации кредитно-финансовой сферы |
| Организовывать процесс сбора информации о событиях риска информационной безопасности организации кредитно-финансовой сферы от структурных подразделений (владельцев риска) организации кредитно-финансовой сферы, а том числе о результатах претензионной работы |
| Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные риски информационной безопасности в рамках бизнес- и технологических процессов организаций кредитно-финансовой сферы |
| Классификация событий риска информационной безопасности организаций кредитно-финансовой сферы |
| Основы организации и ведения баз данных |
| Другие характеристики |  |

## 3.2.4. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка мероприятий, направленных на уменьшение негативного влияния риска информационной безопасности в организациях кредитно-финансовой сферы | Код | B/04.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение способа реагирования на риски информационной безопасности в организации кредитно-финансовой сферы |
| Организация и выполнение работ по разработке плана реагирования на риски информационной безопасности в организации кредитно-финансовой сферы |
| Определение значений контрольных показателей уровня риска в рамках плана реагирования на риск информационной безопасности организации кредитно-финансовой сферы в соответствии с допустимым уровнем такого риска (риск-аппетитом) |
| Определение технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов организации кредитно-финансовой сферы |
| Определение требований к реализации функций безопасности и контролю отсутствия уязвимостей объектов информатизации прикладного уровня |
| Определение организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Разработка мероприятий, направленных на ограничение степени тяжести последствий в результате инцидентов, связанных с реализаций информационных угроз в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать предложения по организации необходимого и достаточного ресурсного (кадрового и финансового) обеспечения процессов системы управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Осуществлять выбор организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Осуществлять выбор технологических мер защиты информации, обрабатываемой в рамках технологических операций, при выполнении бизнес- и технологических процессов в организации кредитно-финансовой сферы |
| Осуществлять планирование деятельности по реагированию на риск информационной безопасности организации кредитно-финансовой сферы |
| Осуществлять планирование процессов подтверждения реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные подходы к реагированию на риск информационной безопасности в организациях кредитно-финансовой сферы |
| Принципы реализации и совершенствования процессов обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Подходы к реализации технологических мер защиты информации, обрабатываемой в рамках технологических операций, при выполнении бизнес- и технологических процессов в организации кредитно-финансовой сферы |
| Подходы к выявлению, реагированию на инциденты информационной безопасности и восстановлению функционирования бизнес- и технологических процессов организации и объектов информатизации кредитно-финансовой сферы |
| Базовый состав организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Классификация событий риска информационной безопасности организаций кредитно-финансовой сферы |
| Принципы и порядок подтверждения реализации функций безопасности и отсутствия уязвимостей в используемых объектах информатизации прикладного уровня |
| Принципы целеполагания, виды и методы организационного планирования |
| Другие характеристики |  |

# 

## 3.2.5. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Мониторинг риска информационной безопасности и контроль показателей уровня риска информационной безопасности в организациях кредитно-финансовой сферы | Код | B/05.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Определение набора ключевых индикаторов риска информационной безопасности в организации кредитно-финансовой сферы |
| Установление требований к ключевым индикаторам риска информационной безопасности в организации кредитно-финансовой сферы |
| Документирование ключевых индикаторов риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация и осуществление деятельности по расчету значений ключевых индикаторов риска информационной безопасности в организации кредитно-финансовой сферы |
| Проведение оценки потенциала превышения сигнальных и контрольных значений контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы |
| Определение порядка реагирования на превышение пороговых значений ключевых индикаторов риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация и выполнение действий по расчету значений контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы |
| Организация и контроль за выполнением мероприятий по переоценке риска информационной безопасности в организации кредитно-финансовой сферы |
| Формирование внутренней отчетности о фактических значениях контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, определяющих набор и требования к ключевым индикаторам риска |
| Применять методологию оценки потенциала превышения сигнальных и контрольных значений показателей уровня риска информационной безопасности в кредитно-финансовой сфере |
| Проводить количественные измерения ключевых индикаторов риска информационной безопасности в кредитно-финансовой сфере |
| Обосновывать пороговые значения ключевых индикаторов риска информационной безопасности в кредитно-финансовой сфере |
| Организовывать сбор информации для расчета ключевых индикаторов риска и контрольных показателей уровня риска информационной безопасности в кредитно-финансовой сфере |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Способы расчета ключевых индикаторов риска информационной безопасности в кредитно-финансовой сфере, в том числе с использованием средств информатизации |
| Подходы к определению состава контрольных показателей уровня риска информационной безопасности в кредитно-финансовой сфере |
| Подходы к организации отчетности в рамках управления рисками информационной безопасности |
| Другие характеристики |  |

# 3.3. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Методологическое обеспечение процессов информационной безопасности в организациях кредитно-финансовой сферы | Код | C | Уровень квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей, профессий | Главный специалист по информационной безопасности  Ведущий специалист по информационной безопасности |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование |
| Требования к опыту практической работы | не менее 3 лет в области информационной безопасности в кредитно-финансовой сфере |
| Особые условия допуска к работе | - |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Главный специалист по технической защите информации |
| ОКПДТР | 20911 | Главный специалист по защите информации |
| ОКСО |  |  |
| 2.09.03.02 | Информационные системы и технологии |
| 2.09.03.03 | Прикладная информатика |
| 2.09.03.04 | Программная инженерия |
| 2.10.03.01 | Информационная безопасность |
| 1.02.04.01 | Математика и компьютерные науки |
| 1.02.04.02 | Фундаментальная информатика и информационные технологии |
| 1.02.04.03 | Математическое обеспечение и администрирование информационных систем |
| 2.09.04.02 | Информационные системы и технологии |
| 2.09.04.03 | Прикладная информатика |
| 2.09.04.04 | Программная инженерия |
| 2.10.04.01 | Информационная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационная безопасность автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |

## 3.3.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации | Код | C/01.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка, согласование и организация утверждения политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Совершенствование политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разработка предложений по распределению ролей и ответственности за управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) в подразделениях, вовлеченных в управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) |
| Разработка предложений по определению зон компетенций Совета директоров (наблюдательного совета) и исполнительного органа организации кредитно-финансовой сферы |
| Разработка предложений по определению состава контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы, а также их контрольных и сигнальных значений |
| Необходимые умения | Анализировать и обосновывать политику организации кредитно-финансовой сферы в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать, вносить предложения по изменению и совершенствованию политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Разрабатывать проекты внутренних документов организации кредитно-финансовой сферы, устанавливающих цели и принципы, а также определяющих методологию и правила по управлению рисками информационной безопасности в организации кредитно-финансовой сферы |
| Разрабатывать предложения по развитию корпоративной культуры (этики), устанавливающей значимость вопросов управления риском информационной безопасности, обеспечения защиты информации, операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Принципы и методы распределения ролей и ответственности за управление рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) |
| Принципы целеполагания, виды и методы организационного планирования |
| Принципы построения и совершенствования систем управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) |
| Принципы разработки политики в области обеспечения информационной безопасности, по вопросам управления риском информационной безопасности, обеспечения операционной надежности (киберустойчивости) и защиты информации |
| Подходы к определению состава контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.3.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | C/02.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка, согласование и применение внутренних документов организации кредитно-финансовой сферы, определяющих методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Совершенствование методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Анализ результатов (валидация) применения методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Разработка программ повышения осведомленности работников организации кредитно-финансовой сферы по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Подготовка предложений по базовому составу организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) организации кредитно-финансовой сферы |
| Методологическое сопровождение реализации программ контроля и аудита защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Определение форматов представления отчетности в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать нормативные правовые акты, национальные и международные документы в части разработки методологии обеспечения информационной безопасности |
| Анализировать и обосновывать методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Разрабатывать внутренние документы организации кредитно-финансовой сферы, определяющие методологию обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Подготавливать информационно-аналитические материалы по вопросам обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы разработки и совершенствования методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы построения систем защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Базовый состав организационных и технических мер по защите информации и обеспечению операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Методология разработки программ повышения осведомленности работников организации кредитно-финансовой сферы по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы организации внутренней отчетности организации кредитно-финансовой сферы в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.3.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка методологии управления рисками информационной безопасности в организациях кредитно-финансовой сферы | Код | C/03.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка, согласование и применение внутренних документов, определяющих методологию управления риском информационной безопасности, в организации кредитно-финансовой сферы |
| Совершенствование методологии управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Анализ результатов (валидация) применения методологии управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Разработка программ повышения осведомленности по вопросам противодействия реализации информационных угроз работников в организации кредитно-финансовой сферы |
| Разработка программ повышения осведомленности по вопросам противодействия реализации информационных угроз в отношении потребителей финансовых услуг |
| Определение форматов представления отчетности в рамках управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Методологическое сопровождение оценки эффективности функционирования системы управления рисками информационной безопасности в организации кредитно-финансовой сферы |
| Разработка методологии оценки риска информационной безопасности в организации кредитно-финансовой сферы |
| Разработка методологии определения потерь от событий риска информационной безопасности |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Анализировать и обосновывать методологию управления рисками информационной безопасности в кредитно-финансовой сфере |
| Разрабатывать внутренние документы организации кредитно-финансовой сферы, определяющие методологию управления рисками информационной безопасности в кредитно-финансовой сфере |
| Подготавливать информационно-аналитические материалы по вопросам управления рисками информационной безопасности в кредитно-финансовой сфере |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Принципы разработки и совершенствования методологии управления рисками информационной безопасности в кредитно-финансовой сфере |
| Принципы построения систем управления рисками информационной безопасности в кредитно-финансовой сфере |
| Методология разработки программ повышения осведомленности по вопросам противодействия реализации информационных угроз в отношении потребителей финансовых услуг |
| Принципы организации внутренней отчетности организации кредитно-финансовой сферы в рамках управления риском информационной безопасности в организации кредитно-финансовой сферы |
| Другие характеристики |  |

## 3.3.4. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Разработка методологии выявления, реагирования и восстановления после инцидентов информационной безопасности в организациях кредитно-финансовой сферы | Код | C/04.7 | Уровень (подуровень) квалификации | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Разработка, согласование внутренних документов, определяющих порядок выявления инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Разработка, согласование внутренних документов, определяющих порядок реагирования на инциденты информационной безопасности в организации кредитно-финансовой сферы |
| Разработка, согласование внутренних документов, определяющих порядок восстановления функционирования бизнес- и технологических процессов и объектов информатизации после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Разработка, согласование внутренних документов, определяющих порядок организации взаимодействия в рамках реагирования на инциденты информационной безопасности в организации кредитно-финансовой сферы |
| Разработка, согласование внутренних документов, определяющих порядок проведения анализа причин и последствий реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Определение показателей эффективности реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Разработка, согласование внутренних документов, определяющих методологию оценки потенциала влияния (критичности) инцидента информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Обеспечивать методологическое сопровождение деятельности организации кредитно-финансовой сферы в части выявления, реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Разрабатывать внутренние документы организации кредитно-финансовой сферы |
| Подготавливать информационно-аналитические материалы по вопросам выявления, реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основы организации процессов выявления, реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Ключевые показатели эффективности деятельности организации кредитно-финансовой сферы по выявлению, реагированию и восстановлению после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Форматы обмена информацией об инцидентах информационной безопасности в организации кредитно-финансовой сферы |
| Принципы и методы распределения ролей и ответственности в рамках реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Основные подходы и лучшие практики по сбору технических данных (свидетельств) в рамках выявления, реагирования и восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Другие характеристики |  |

## .

# 3.4. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Обеспечение информационной безопасности в организациях кредитно-финансовой сферы | Код | D | Уровень квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Специалист по информационной безопасности  Специалист по информационной безопасности 2-й категории  Специалист по информационной безопасности 1-й категории |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | - |
| Другие характеристики | Для должностей с категорией – опыт работы в должности с более низкой (предшествующей) категорией не менее двух лет |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Инженер-программист по технической защите информации |
| - | Инженер по защите информации |
| - | Администратор по обеспечению безопасности информации |
| - | Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры |
| ОКПДТР | 22567 | Инженер по защите информации |
| 26579 | Специалист по защите информации |
| ОКСО |  |  |
| 2.09.03.02 | Информационные системы и технологии |
| 2.09.03.03 | Прикладная информатика |
| 2.09.03.04 | Программная инженерия |
| 2.10.03.01 | Информационная безопасность |
| 1.02.04.01 | Математика и компьютерные науки |
| 1.02.04.02 | Фундаментальная информатика и информационные технологии |
| 1.02.04.03 | Математическое обеспечение и администрирование информационных систем |
| 2.09.04.02 | Информационные системы и технологии |
| 2.09.04.03 | Прикладная информатика |
| 2.09.04.04 | Программная инженерия |
| 2.10.04.01 | Информационная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационная безопасность автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |

## 3.4.1. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Реализация процессов защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | D/01.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Реализация и совершенствование процессов применения технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов |
| Реализация и совершенствование процессов реализации функций безопасности и контроля отсутствия уязвимостей объектов информатизации прикладного уровня |
| Реализация и совершенствование организационных и технологических мер по защите информации и обеспечению операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Реализация и совершенствование процессов обеспечения защиты информации и операционной надежности (киберустойчивости) на этапах жизненного цикла объектов информатизации прикладного уровня |
| Обеспечение необходимого уровня зрелости (полноты и качества) обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Реализация контуров безопасности в рамках обеспечения защиты информации в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать предложения по совершенствованию методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Применять технологические меры для обеспечения защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов |
| Применять организационные и технические меры защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Вносить предложения по изменению состава контрольных показателей уровня риска информационной безопасности в организации кредитно-финансовой сферы |
| Анализировать техническую документацию на объекты информатизации |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Базовый состав организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Подходы к сегментации вычислительных сетей |
| Основы обеспечения безопасности объектов информатизации прикладного уровня |
| Подходы к подтверждению реализации функций безопасности и контроля отсутствия уязвимостей объектов информатизации прикладного уровня |
| Другие характеристики |  |

## 3.4.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы | Код | D/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Контроль реализации процессов применения технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов в организации кредитно-финансовой сферы |
| Контроль за выполнением процессов реализации функций безопасности и контроля отсутствия уязвимостей объектов информатизации прикладного уровня |
| Контроль реализацией организационных и технологических мер по защите информации и обеспечению операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Контроль реализации процессов обеспечения защиты информации и операционной надежности (киберустойчивости) на этапах жизненного цикла объектов информатизации прикладного уровня |
| Реализация программ контроля и аудита защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Представление отчетности в рамках обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Организация и проведение сценарного анализа и тестирования готовности организации кредитно-финансовой сферы противостоять реализации информационных угроз |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Разрабатывать предложения по совершенствованию методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Применять технологические меры защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов |
| Применять организационные и технические меры защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Анализировать техническую документацию на объекты информатизации |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере реализации и контроля процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Базовый состав организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Подходы к сегментации вычислительных сетей |
| Основы обеспечения безопасности объектов информатизации прикладного уровня |
| Другие характеристики |  |

## 3.4.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Реализация программ повышения осведомленности по вопросам противодействия реализации информационных угроз в организациях кредитно-финансовой сферы | Код | D/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Организация инструктажа работников организации кредитно-финансовой сферы в соответствии с программами повышения осведомленности |
| Организация мероприятий по повышению осведомленности работников по вопросам организации и контроля за управлением риском информационной безопасности, защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Проведение контрольных мероприятий по результатам реализации программ повышения осведомленности работников организации кредитно-финансовой сферы по вопросам противодействия реализации информационных угроз |
| Организация мероприятий по повышению осведомленности и проведение инструктажа работников, входящих в группы повышенного риска, по вопросам выявления и противодействия реализации информационных угроз в организации кредитно-финансовой сферы |
| Подготовка предложений по совершенствованию программ повышения осведомленности в организации кредитно-финансовой сферы |
| Информирование потребителей финансовых услуг, направленное на уменьшение негативного влияния риска информационной безопасности |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Организовывать и проводить мероприятия по повышению осведомленности |
| Применять технологические меры защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов |
| Применять организационные и технические меры защиты информации и обеспечения операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Принципы обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Основы обеспечения безопасности объектов информатизации прикладного уровня |
| Другие характеристики |  |

# 3.5. Обобщенная трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Управление инцидентами информационной безопасности в организациях кредитно-финансовой сферы | Код | F | Уровень квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение обобщенной трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Возможные наименования должностей | Специалист по информационной безопасности  Специалист по информационной безопасности 2-й категории  Специалист по информационной безопасности 1-й категории |

|  |  |
| --- | --- |
| Требования к образованию и обучению | Высшее образование |
| Требования к опыту практической работы | - |
| Особые условия допуска к работе | - |
| Другие характеристики | Для должностей с категорией – опыт работы в должности с более низкой (предшествующей)  категорией не менее двух лет |

Дополнительные характеристики

|  |  |  |
| --- | --- | --- |
| Наименование документа | Код | Наименование базовой группы, должности (профессии) или специальности |
| ОКЗ | 2529 | Специалисты по базам данных и сетям, не входящие в другие группы |
| ЕКС | - | Инженер-программист по технической защите информации |
| - | Инженер по защите информации |
| - | Администратор по обеспечению безопасности информации |
| - | Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры |
| ОКПДТР | 22567 | Инженер по защите информации |
| 26579 | Специалист по защите информации |
| ОКСО |  |  |
| 2.09.03.02 | Информационные системы и технологии |
| 2.09.03.03 | Прикладная информатика |
| 2.09.03.04 | Программная инженерия |
| 2.10.03.01 | Информационная безопасность |
| 1.02.04.01 | Математика и компьютерные науки |
| 1.02.04.02 | Фундаментальная информатика и информационные технологии |
| 1.02.04.03 | Математическое обеспечение и администрирование информационных систем |
| 2.09.04.02 | Информационные системы и технологии |
| 2.09.04.03 | Прикладная информатика |
| 2.09.04.04 | Программная инженерия |
| 2.10.04.01 | Информационная безопасность |
| 2.10.05.02 | Информационная безопасность телекоммуникационных систем |
| 2.10.05.03 | Информационная безопасность автоматизированных систем |
| 2.10.05.04 | Информационно-аналитические системы безопасности |
| 2.10.05.05 | Безопасность информационных технологий в правоохранительной сфере |

## 3.5.1. Трудовая функция

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Оперативный мониторинг и выявление событий информационной безопасности в организации кредитно-финансовой сферы |
| Сбор данных для регистрации событий информационной безопасности в организации кредитно-финансовой сферы |
| Обеспечение функционирования механизмов и инициативного информирования работниками организации кредитно-финансовой сферы о событиях информационной безопасности в организации кредитно-финансовой сферы |
| Организация и выполнение деятельности по получению и использованию сведений об актуальных индикаторах компрометации объектов информатизации в организации кредитно-финансовой сферы |
| Автоматизация процедур выявления наличия индикаторов компрометации в организации кредитно-финансовой сферы |
| Сбор и регистрация информации об инцидентах информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Настраивать средства (агентов, интерфейсов) сбора технических данных для выявления событий информационной безопасности в организации кредитно-финансовой сферы |
| Осуществлять работу с техническими средствами, реализующими функции управления инцидентами защиты информации в организации кредитно-финансовой сферы |
| Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Формировать отчетность о выявленных событиях и инцидентах информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные уязвимости и информационные угрозы, характерные для организаций кредитно-финансовой сферы |
| Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в организации кредитно-финансовой сферы |
| Подходы к настройке средств сбор технических данных для выявления событий инцидентов информационной безопасности в организации кредитно-финансовой сфере |
| Типовые события и инциденты информационной безопасности в организации кредитно-финансовой сферы |
| Подходы к описанию сценариев реализации инцидентов информационной безопасности в организации кредитно- финансовой сферы |
| Другие характеристики |  |

## 3.5.2. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Реагирование на инциденты информационной безопасности | Код | F/02.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Реализация порядка реагирования на инциденты информационной безопасности в организации кредитно-финансовой сферы |
| Сбор информации об инцидентах информационной безопасности, их классификация и оценка потенциала влияния (критичности) в организации кредитно-финансовой сферы |
| Выполнение действий по реагированию на инциденты информационной безопасности в соответствии с едиными правилами и процедурами реагирования на такие инциденты в организации кредитно-финансовой сферы |
| Разработка единых правил и процедур реагирования на инциденты информационной безопасности в организации кредитно-финансовой сферы |
| Осуществление взаимодействия в рамках реагирования на инциденты информационной безопасности в организации кредитно-финансовой сферы, а также во взаимодействии с внешними заинтересованными организациями |
| Информирование Банка России и федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, об инцидентах информационной безопасности в организации кредитно-финансовой сферы в соответствии с определенными формами и сроками |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Настраивать средства (агентов, интерфейсов) сбора технических данных для выявления событий информационной безопасности |
| Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Анализировать технические данные, свидетельствующие о возникновении событий информационной безопасности в организации кредитно-финансовой сферы |
| Формировать отчетность о выявленных событиях и инцидентах информационной безопасности в организации кредитно-финансовой сферы |
| Работать с техническими средствами, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Применять меры, направленные на снижение тяжести последствий от реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Применять методологию оценки потенциала влияния (критичности) инцидента информационной безопасности организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы. |
| Основные уязвимости и информационные угрозы, характерные для организаций кредитно-финансовой сферы |
| Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности в кредитно-финансовой сфере |
| Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в кредитно-финансовой сфере |
| Подходы к настройке средств сбор технических данных для выявления событий инцидентов информационной безопасности в кредитно-финансовой сфере |
| Типовые события и инциденты информационной безопасности в кредитно-финансовой сфере |
| Принципы работы с техническими средствами, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Подходы к описанию сценариев реализации инцидентов информационной безопасности в организации кредитно- финансовой сферы |
| Другие характеристики |  |

## 3.5.3. Трудовая функция

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Восстановление после реализации инцидентов информационной безопасности | Код | F/03.6 | Уровень (подуровень) квалификации | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Происхождение трудовой функции | Оригинал | X | Заимствовано из оригинала |  |  |  |
|  |  |  |  |  | Код оригинала | Регистрационный номер профессионального стандарта |

|  |  |
| --- | --- |
| Трудовые действия | Реализация порядка восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Выполнение действий по восстановлению после инцидентов информационной безопасности в соответствии с едиными правилами и процедурами после реализации таких инцидентов в организации кредитно-финансовой сферы |
| Разработка единых правил и процедур по восстановлению после инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Определение критериев для оценки завершения восстановления и условий закрытия инцидента информационной безопасности в организации кредитно-финансовой сферы |
| Проведение оценки завершения восстановления для закрытия инцидента информационной безопасности в организации кредитно-финансовой сферы |
| Сбор и фиксация технических данных (свидетельств) в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Осуществление взаимодействия в рамках восстановления после инцидентов информационной безопасности в организации кредитно-финансовой сферы, а также с внешними заинтересованными организациями |
| Информирование Банка России и 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 организации кредитно-финансовой сферы |
| Необходимые умения | Анализировать и применять действующую нормативно-правовую и методологическую базу, а также требования законодательства Российской Федерации и нормативных актов Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) |
| Осуществлять работу с техническими средствами защиты информации, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Анализировать технические данные, свидетельствующие о возникновении событий и инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Формировать отчетность в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности |
| Работать с техническими средствами, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Применять меры, направленные на снижение тяжести последствий от реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Необходимые знания | Законодательство Российской Федерации, нормативные акты Банка России, международные и национальные стандарты в сфере управления рисками информационной безопасности, обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях кредитно-финансовой сферы |
| Основные уязвимости и информационные угрозы, характерные для организаций кредитно-финансовой сферы |
| Базовый состав и функциональные возможности технических средств сбора технических данных для выявления событий и инцидентов информационной безопасности в кредитно-финансовой сфере |
| Принципы построения систем обеспечения защиты информации и операционной надежности (киберустойчивости) в кредитно-финансовой сфере |
| Типовые события и инциденты информационной безопасности в кредитно-финансовой сфере |
| Принципы работы с техническими средствами, реализующими функции управления инцидентами информационной безопасности организации кредитно-финансовой сферы |
| Подходы к описанию сценариев реализации инцидентов информационной безопасности в организации кредитно-финансовой сферы |
| Другие характеристики |  |

IV. Сведения об организациях – разработчиках профессионального стандарта

**4.1. Ответственная организация-разработчик**

|  |
| --- |
| Центральный банк Российской Федерации |
|  |

**4.2. Наименования организаций-разработчиков**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

1. «ОК 010-2014 (МСКЗ-08). Общероссийский классификатор занятий» (принят и введен в действие приказом Росстандарта от 12.12.2014 № 2020-ст). [↑](#endnote-ref-1)
2. Общероссийский классификатор видов экономической деятельности. [↑](#endnote-ref-2)
3. «ОК 009-2016. Общероссийский классификатор специальностей по образованию» (принят и введен в действие приказом Росстандарта от 08.12.2016 № 2007-ст). [↑](#endnote-ref-3)