\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Должностная инструкция**  
**инженера информационной безопасности**  
**службы информационных технологий**

УТВЕРЖДАЮ

Главный врач

\_\_\_\_\_\_\_\_\_\_\_

«\_\_» \_\_\_\_\_\_ 20\_\_ года

**1. Общие положения**

1.1. Настоящая должностная инструкция определяет должностные обязанности, права и ответственность инженера информационной безопасности службы информационных технологий (далее – специалист).

1.2. На должность специалиста принимается лицо:

1.2.1. Имеющее высшее образование – бакалавриат в области информационной безопасности, либо высшее образование – специалитет или магистратура в области информационной безопасности.

1.2.2. Имеющее допуск к государственной тайне (при необходимости).

1.2.3. Проходящее дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3. Инженер информационной безопасности службы информационных технологий в своей работе руководствуется:

* действующим законодательством РФ;
* Трудовым кодексом РФ;
* нормативно-правовыми и инструктивно-методическими документами по специфике деятельности;
* Уставом медицинской организации;
* приказами и распоряжениями (в том числе устными) главного врача медицинской организации, директора службы информационных технологий;
* планами работ, утвержденными главным врачом медицинской организации;
* действующими в медицинской организации правилами внутреннего трудового распорядка;
* требованиями охраны труда, пожарной безопасности, информационной безопасности;
* Руководством по качеству;
* настоящей должностной инструкцией;
* другой действующей документацией системы менеджмента качества в медицинской организации.

1.4. Специалист назначается и освобождается от занимаемой должности приказом главного врача медицинской организации по представлению директора службы информационных технологий.

1.5. Специалист непосредственно подчиняется директору службы информационных технологий.

1.6. Специалист должен знать:

1.6.1. В рамках трудовой функции «Администрирование подсистем защиты информации в операционных системах»:

архитектура и принципы построения операционных систем

программные интерфейсы операционных систем

виды политик управления доступом и информационными потоками применительно к операционным системам

* архитектуру подсистем защиты информации в операционных системах;
* принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы;
* состав типовых конфигураций программно-аппаратных средств защиты информации;
* требования по составу и характеристикам подсистем защиты информации применительно к операционным системам;
* порядок реализации методов и средств антивирусной защиты в операционных системах;
* программно-аппаратные средства и методы защиты информации в операционных системах;
* принципы работы и правила эксплуатации программно-аппаратных средств защиты информации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.2. В рамках трудовой функции «Администрирование программно-аппаратных средств защиты информации в компьютерных сетях»:

* принципы построения компьютерных сетей;
* стек сетевых протоколов операционных систем;
* стек протоколов сетевого оборудования;
* порядок реализации методов и средств межсетевого экранирования;
* принципы функционирования сетевых протоколов, включающих криптографические алгоритмы;
* виды политик управления доступом и информационными потоками в компьютерных сетях;
* источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;
* состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
* методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;
* принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;
* программно-аппаратные средства и методы защиты информации в компьютерных сетях;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.3. В рамках трудовой функции «Администрирование средств защиты информации прикладного и системного программного обеспечения»:

* архитектуру подсистем защиты информации в операционных системах;
* принципы построения систем управления базами данных;
* основные средства и методы анализа программных реализаций;
* принципы построения антивирусного программного обеспечения;
* виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению;
* источники угроз информационной безопасности программного обеспечения и меры по их предотвращению;
* уязвимости используемого программного обеспечения и методы их эксплуатации;
* виды и формы функционирования вредоносного программного обеспечения;
* характерные признаки наличия вредоносного программного обеспечения;
* средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения;
* принципы функционирования программных средств криптографической защиты информации;
* порядок обеспечения безопасности информации при эксплуатации программного обеспечения;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.4. В рамках трудовой функции «Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»:

* принципы построения компьютерных систем и сетей;
* методы и методики оценки безопасности программно-аппаратных средств защиты информации;
* принципы построения программно-аппаратных средств защиты информации;
* принципы построения подсистем защиты информации в компьютерных системах;
* методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации;
* методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации;
* методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей;
* способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности;
* национальные, межгосударственные и международные стандарты в области защиты информации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.5. В рамках трудовой функции «Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей»:

* принципы построения компьютерных систем и сетей;
* модели безопасности компьютерных систем;
* виды политик безопасности компьютерных систем и сетей;
* принципы построения средств криптографической защиты информации;
* национальные, межгосударственные и международные стандарты в области защиты информации;
* возможности используемых и планируемых к использованию средств защиты информации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.6. В рамках трудовой функции «Проведение анализа безопасности компьютерных систем»:

* принципы построения компьютерных систем и сетей;
* уязвимости компьютерных систем и сетей;
* криптографические методы защиты информации;
* принципы построения систем управления базами данных;
* средства анализа конфигураций;
* национальные, межгосударственные и международные стандарты в области защиты информации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.7. В рамках трудовой функции «Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов»:

* национальные, межгосударственные и международные стандарты в области защиты информации;
* национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации;
* способы организации работ при проведении сертификации программно-аппаратных средств защиты;
* принципы построения средств криптографической защиты информации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.8. В рамках трудовой функции «Проведение инструментального мониторинга защищенности компьютерных систем и сетей»:

* принципы построения компьютерных систем и сетей;
* формальные модели безопасности компьютерных систем и сетей;
* принципы построения систем обнаружения компьютерных атак;
* методы обработки данных мониторинга безопасности компьютерных систем и сетей;
* порядок создания и структура отчета, создаваемого по результатам проверок;
* способы обнаружения и нейтрализации последствий вторжений в компьютерные системы;
* криптографические протоколы, применяемые в компьютерных сетях;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.6.9. В рамках трудовой функции «Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов»:

* форматы хранения информации в анализируемой компьютерной системе;
* основные форматы файлов, используемые в компьютерных системах;
* особенности хранения конфигурационной и системной информации в компьютерных системах;
* уязвимости компьютерных систем и сетей;
* технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов;
* порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;
* нормы уголовного и административного права в сфере компьютерной информации;
* характеристики правонарушений в области связи и информации;
* виды преступлений в сфере компьютерной информации;
* порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
* способы обнаружения и нейтрализации последствий вторжений в компьютерные системы;
* методы анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении;
* порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;
* методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;
* методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов;
* криптографические алгоритмы и особенности их программной реализации;
* нормативные правовые акты в области защиты информации;
* руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
* организационные меры по защите информации.

1.7. Специалист должен уметь:

1.7.1. В рамках трудовой функции «Администрирование подсистем защиты информации в операционных системах»:

* формулировать политики безопасности операционных систем;
* настраивать политики безопасности операционных систем;
* оценивать угрозы безопасности информации операционных систем;
* противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем;
* выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах;
* настраивать антивирусные средства защиты информации в операционных системах;
* устанавливать обновления программного обеспечения и средств антивирусной защиты;
* проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах;
* производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах;
* оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

1.7.2. В рамках трудовой функции «Администрирование программно-аппаратных средств защиты информации в компьютерных сетях»:

* оценивать угрозы безопасности информации в компьютерных сетях;
* настраивать правила фильтрации пакетов в компьютерных сетях;
* обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;
* конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;
* выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;
* проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
* производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях;
* оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.

1.7.3. В рамках трудовой функции «Администрирование средств защиты информации прикладного и системного программного обеспечения»:

* анализировать угрозы безопасности информации программного обеспечения;
* формулировать правила безопасной эксплуатации программного обеспечения;
* обосновывать правила безопасной эксплуатации программного обеспечения;
* анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия;
* производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации;
* осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения;
* определять порядок функционирования программного обеспечения с целью обеспечения защиты информации;
* анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.

1.7.4. В рамках трудовой функции «Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»:

* определять параметры функционирования программно-аппаратных средств защиты информации;
* разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации;
* оценивать эффективность защиты информации;
* применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации;
* анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия.

1.7.5. В рамках трудовой функции «Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей»:

* анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;
* разрабатывать профили защиты компьютерных систем;
* формулировать задания по безопасности компьютерных систем;
* выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации;
* формировать политики безопасности компьютерных систем и сетей.

1.7.6. В рамках трудовой функции «Проведение анализа безопасности компьютерных систем»:

* анализировать компьютерную систему с целью определения уровня защищенности и доверия;
* прогнозировать возможные пути развития действий нарушителя информационной безопасности;
* производить анализ политики безопасности на предмет адекватности;
* проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;
* составлять и оформлять аналитический отчет по результатам проведенного анализа;
* разрабатывать предложения по устранению выявленных уязвимостей.

1.7.7. В рамках трудовой функции «Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов»:

* анализировать компьютерную систему с целью определения уровня защищенности и доверия;
* использовать профили защиты и задания по безопасности;
* применять инструментальные средства проведения сертификационных испытаний;
* составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям;
* делать выводы по оценке защищенности на основании аналитического отчета.

1.7.8. В рамках трудовой функции «Проведение инструментального мониторинга защищенности компьютерных систем и сетей»:

* формализовывать задачу управления безопасностью компьютерных систем;
* применять инструментальные средства проведения мониторинга защищенности компьютерных систем;
* применять методы анализа защищенности компьютерных систем и сетей;
* структурировать аналитическую информацию для включения в отчет.

1.7.9. В рамках трудовой функции «Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов»:

* применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа;
* анализировать структуру механизма возникновения и обстоятельства события;
* определять причину и условия изменения программного обеспечения;
* выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
* определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой;
* применять действующую законодательную базу в области обеспечения защиты информации;
* выявлять возможные траектории состояний функционирования системы;
* выявлять несоответствия имеющейся информации ее расположению в системе;
* прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов.

**2. Должностные обязанности**

2.1. В рамках трудовой функции «Администрирование подсистем защиты информации в операционных системах»:

* определение состава применяемых программно-аппаратных средств защиты информации в операционных системах;
* разработка порядка применения программно-аппаратных средств защиты информации в операционных системах;
* формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах;
* установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации;
* конфигурирование программно-аппаратных средств защиты информации в операционных системах;
* контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах;
* управление антивирусной защитой операционных систем в соответствии с действующими требованиями.

2.2. В рамках трудовой функции «Администрирование программно-аппаратных средств защиты информации в компьютерных сетях»:

* определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях;
* разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях;
* формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях;
* настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации;
* управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях;
* контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
* управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.

2.3. В рамках трудовой функции «Администрирование средств защиты информации прикладного и системного программного обеспечения»:

* определение порядка установки программного обеспечения с целью соблюдения требований по защите информации;
* контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение;
* формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения;
* выполнение работ по обнаружению вредоносного программного обеспечения;
* ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования;
* формулирование требований к встроенным средствам защиты информации программного обеспечения.

2.4. В рамках трудовой функции «Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»:

* оценка работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик;
* оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик;
* определение уровня защищенности и доверия программно-аппаратных средств защиты информации.

2.5. В рамках трудовой функции «Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей»:

* формирование политик безопасности компьютерных систем;
* консультирование по вопросам безопасности компьютерных систем;
* разработка профилей защиты и заданий по безопасности;
* разработка технических заданий на создание средств защиты информации;
* принятие решения о необходимости защиты информации, содержащейся в информационной системе;
* классификация информационной системы по требованиям защиты информации;
* определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети;
* разработка модели угроз безопасности информации;
* задание требований к защите информации компьютерной системы;
* разработка руководящих документов по защите информации в организации.

2.6. В рамках трудовой функции «Проведение анализа безопасности компьютерных систем»:

* определение уровня защищенности и доверия в компьютерных системах;
* оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем;
* оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам;
* подготовка аналитического отчета по результатам проведенного анализа;
* формулирование предложений по устранению выявленных уязвимостей.

2.7.  В рамках трудовой функции «Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов»:

* проведение теоретических исследований уровней защищенности компьютерных систем и сетей;
* проведение экспериментальных исследований уровней защищенности компьютерных систем и сетей;
* проведение сертификационных испытаний с использованием инструментальных средств;
* подготовка аналитического отчета по результатам проведенных сертификационных испытаний;
* формулирование выводов по оценке защищенности.

2.8. В рамках трудовой функции «Проведение инструментального мониторинга защищенности компьютерных систем и сетей»:

* выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности;
* выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;
* составление отчетов по результатам проверок.

2.9. В рамках трудовой функции «Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов»:

* определение свойств аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния;
* классификация свойств аппаратных средств в составе компьютерной системы;
* диагностика причин, условий изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы;
* определение характеристик операционной системы и используемых технологий системного программирования;
* анализ функциональных свойств программного обеспечения;
* исследование алгоритма программного продукта и типов поддерживаемых аппаратных платформ;
* определение причин, целей и условий изменения свойств (состояния) программного обеспечения;
* индивидуальное отождествление оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы;
* установление групповой принадлежности программного обеспечения;
* выработка предложений по устранению выявленных уязвимостей;
* выявление индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы;
* установление вида, свойств и состояния информации (фактического и первоначального, в том числе до ее удаления и модификации) в компьютерной системе;
* определение причин и условий изменения свойств исследуемой информации;
* определение механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям;
* установление участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация;
* установление соответствия либо несоответствия действий с информацией специальному регламенту (правилам);
* составление экспертного заключения.

**3.** **Права**

Инженер информационной безопасности службы информационных технологий для выполнения своих функций наделяется следующими полномочиями:

3.1. Знакомиться с проектами решений руководства предприятия, касающихся его деятельности.

3.2. Вносить на рассмотрение руководства предложений по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности организации (ее структурных подразделениях) и вносить предложения по их устранению.

3.4. Запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.

3.5. Привлекать специалистов отдельных структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет – то с разрешения их руководителей).

3.6. Требовать от своего непосредственного руководителя, руководства предприятия оказания содействия в исполнении им своих должностных обязанностей  
и прав.

**4. Ответственность**

4.1. Инженер информационной безопасности службы информационных технологий несет ответственность за:

4.1.1 Своевременное и качественное осуществление возложенных на него должностных обязанностей.

4.1.2. Организацию своей работы, своевременное и квалифицированное выполнение приказов, распоряжений и поручений главного врача клиники и руководителя соответствующего подразделения, нормативно-правовых актов по своей деятельности.

4.1.3. Рациональное и эффективное использование материальных, финансовых  
и кадровых ресурсов.

4.1.4. Соблюдение правил внутреннего распорядка, санитарно-противоэпидемического режима, противопожарной безопасности и техники безопасности.

4.1.5. Ведение документации, предусмотренной действующими нормативно-правовыми актами.

4.1.6. Представление в установленном порядке статистической и иной информации по своей деятельности и деятельности подразделения.

4.1.7. Обеспечение подразделения к работе в условиях чрезвычайных ситуаций.

4.2. За нарушение трудовой дисциплины, законодательных и нормативно-правовых актов инженер информационной безопасности службы информационных технологий может быть привлечен в соответствии с действующим законодательством в зависимости от тяжести проступка к дисциплинарной, материальной, административной и уголовной ответственности.

Настоящая должностная инструкция инженера информационной безопасности службы информационных технологий разработана в соответствии с профессиональным стандартом «Специалист по безопасности компьютерных систем и сетей» (приказ Минтруда от 01.11.2016 № 598н), Трудовым кодексом, трудовым договором, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и другими нормативными актами, регулирующими трудовые отношения между работником и работодателем.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |
|  |  |  |
| Согласовано: |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |
| Ознакомлен: |  |  |
| Инженер информационной безопасности службы информационных технологий | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |