ПРИЛОЖЕНИЕ 1

**УТВЕРЖДЕН**

**ПМ.02 Осуществление интеграции программных модулей**

**Проектирование модулей системы защиты объекта критической информационной инфраструктуры (КИИ) на основе 187-ФЗ «О безопасности КИИ Российской Федерации»**

**Техническое задание**

**Листов 17**

|  |  |
| --- | --- |
| **Инв. № подл** |  |
| **Подпись и дата** |  |
| **Взам. инв. №** |  |
| **Инв. № дубл.** |  |
| **Подпись и дата** |  |

**2024**

**СОДЕРЖАНИЕ**

[**1. ВВЕДЕНИЕ 2**](#_Toc165013159)

[**2. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ 3**](#_Toc165013160)

[**3. НАЗНАЧЕНИЕ РАЗРАБОТКИ 4**](#_Toc165013161)

[**4. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ 5**](#_Toc165013162)

[**4.1. Требования к функциональным характеристикам 5**](#_Toc165013163)

[**4.2. Требования к надежности 5**](#_Toc165013164)

[**4.3. Условия эксплуатации 6**](#_Toc165013165)

[**4.4. Требования к составу и параметрам технических средств 7**](#_Toc165013166)

[**4.5. Требования к информационной и программной совместимости 8**](#_Toc165013167)

[**4.6. Требования к маркировке и упаковке 9**](#_Toc165013168)

[**4.7. Требования к транспортированию и хранению 10**](#_Toc165013169)

[**4.8. Специальные требования 10**](#_Toc165013170)

[**5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ 11**](#_Toc165013171)

[**6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ 12**](#_Toc165013172)

[**7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ 13**](#_Toc165013173)

[**8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ 14**](#_Toc165013174)

# **ВВЕДЕНИЕ**

На фоне быстрого развития информационных технологий и усиления киберугроз, обеспечение безопасности информации и защиты от несанкционированного доступа становится одним из ключевых приоритетов для организаций, особенно в сфере обороны. В связи с этим, разработка программного решения для системы централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий, получившей название "Стражник", становится необходимой и актуальной задачей. Целью данного технического задания является создание интегрированной системы мониторинга, обеспечивающей непрерывный анализ активности на рабочих станциях, выявление потенциальных угроз и инцидентов безопасности, а также оперативное реагирование на них. Программное решение "Стражник" предназначено для обеспечения высокого уровня защиты конфиденциальной информации, важных ресурсов и сетевой инфраструктуры организаций в сфере обороны. Данное техническое задание определяет основные требования к функциональности, архитектуре, безопасности и производительности программного решения "Стражник", а также устанавливает основные этапы его разработки, интеграции и внедрения. В ходе выполнения задания предполагается тесное взаимодействие с заказчиком для уточнения требований и обеспечения полного соответствия разрабатываемого решения поставленным задачам и ожиданиям пользователей. Реализация программного решения "Стражник" позволит значительно повысить уровень информационной безопасности в организациях, работающих в сфере обороны, и обеспечить эффективное реагирование на угрозы и инциденты безопасности, минимизируя потенциальные убытки и риски.

# **ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ**

С учетом быстрого развития информационных технологий и увеличения угроз в сфере кибербезопасности, необходимость обеспечения защиты информации и данных становится стратегически важной для организаций, особенно для тех, что занимаются вопросами обороны и безопасности. Министерство обороны Российской Федерации и оборонные предприятия, в своей деятельности, имеют дело с чрезвычайно чувствительной информацией, требующей надежной защиты от утечек и несанкционированного доступа. В контексте постоянно возрастающих киберугроз и разнообразных способов атак, стандартные методы обеспечения безопасности уже недостаточны. Однако, с развитием технологий также возникают и новые возможности для защиты информации. Создание программного решения, такого как "Стражник", который будет обеспечивать централизованный мониторинг событий на рабочих станциях сотрудников Министерства обороны Российской Федерации и оборонных предприятий, представляется важным шагом для обеспечения безопасности информации и данных. Основываясь на вышесказанном, разработка программного решения "Стражник" является необходимой мерой для защиты конфиденциальной информации, ресурсов и сетевой инфраструктуры в сфере обороны. Это программное решение будет способствовать обнаружению и предотвращению потенциальных угроз, а также обеспечит оперативное реагирование на инциденты безопасности, что в конечном итоге поможет сократить возможные убытки и риски для организаций и страны в целом

# **НАЗНАЧЕНИЕ РАЗРАБОТКИ**

Целью данного технического задания является разработка программного решения "Стражник" - системы централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий. Это решение направлено на обеспечение непрерывного анализа активности на рабочих станциях, выявление потенциальных угроз и инцидентов безопасности, а также оперативное реагирование на них. Главной целью разработки является повышение уровня защиты конфиденциальной информации, важных ресурсов и сетевой инфраструктуры в сфере обороны. Реализация программного решения "Стражник" позволит существенно усилить меры безопасности и обеспечить эффективное реагирование на угрозы, что, в свою очередь, поможет минимизировать потенциальные убытки и риски для организаций и страны в целом. Таким образом, разработка "Стражника" имеет стратегическое значение для обеспечения безопасности информации и защиты от киберугроз в секторе обороны, подтверждая принятие организациями ответственного подхода к защите конфиденциальных данных и инфраструктуры.

# **4. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ**

## **4.1. Требования к функциональным характеристикам**

Программное решение "Стражник" должно обладать следующими функциональными характеристиками:

1. **Централизованный мониторинг событий**: Система должна способствовать сбору, анализу и отслеживанию всех событий, происходящих на рабочих станциях сотрудников Министерства обороны Российской Федерации и оборонных предприятий. Это включает в себя мониторинг доступа к данным, сетевой активности, а также любых других действий, связанных с безопасностью информации.
2. **Выявление потенциальных угроз**: Программа должна иметь возможность обнаруживать необычное или подозрительное поведение на рабочих станциях, которое может указывать на возможные киберугрозы или нарушения безопасности.
3. **Оперативное реагирование**: "Стражник" должен предоставлять механизмы оперативного реагирования на обнаруженные угрозы. Это может включать в себя автоматические реакции, оповещения безопасностных администраторов или иные меры, направленные на предотвращение ущерба от потенциальных инцидентов.
4. **Гибкость и масштабируемость**: Система должна быть гибкой и масштабируемой, чтобы адаптироваться к изменяющимся потребностям и объемам данных. Это включает в себя возможность добавления новых функций, поддержку различных типов рабочих станций и способность обрабатывать большие объемы информации.
5. **Интеграция с существующими системами безопасности**: Программное решение должно без проблем интегрироваться с уже существующими системами безопасности и инфраструктурой министерства обороны и оборонных предприятий.
6. **Защита данных и конфиденциальность**: "Стражник" должен обеспечивать высокий уровень защиты данных и конфиденциальности, предотвращая несанкционированный доступ к информации и обеспечивая ее целостность.
7. **Удобный интерфейс и отчетность**: Программа должна иметь понятный и удобный интерфейс для администраторов безопасности, а также предоставлять возможность генерации отчетов о произошедших событиях и действиях по обеспечению безопасности.

## **4.2. Требования к надежности**

Важным аспектом программного решения "Стражник" является его надежность, поскольку система должна функционировать без сбоев и обеспечивать постоянную защиту конфиденциальной информации. Ниже перечислены требования к надежности:

1. **Отказоустойчивость**: Система должна быть спроектирована с учетом возможных отказов и сбоев, чтобы минимизировать вероятность простоев и обеспечить непрерывную работу в любых условиях.
2. **Резервное копирование и восстановление**: "Стражник" должен иметь механизмы регулярного резервного копирования данных и возможность быстрого восстановления после сбоев или чрезвычайных ситуаций.
3. **Тестирование и отладка**: перед внедрением системы необходимо провести тщательное тестирование всех ее компонентов и функций, а также обеспечить наличие механизмов для быстрого обнаружения и устранения ошибок.
4. **Мониторинг состояния системы**: для обеспечения надежной работы системы необходимо регулярно мониторить ее состояние, производительность и загрузку, чтобы своевременно выявлять и устранять потенциальные проблемы.
5. **Защита от внешних атак и вмешательств**: "Стражник" должен иметь механизмы защиты от внешних киберугроз, включая атаки хакеров, вирусы и другие виды вредоносного программного обеспечения.
6. **Обновление и поддержка**: Система должна регулярно обновляться и поддерживаться разработчиками для обеспечения безопасности и соответствия современным стандартам и требованиям.
7. **Документация и обучение персонала**: для обеспечения надежной эксплуатации системы необходимо предоставить подробную документацию по ее установке, настройке и использованию, а также обеспечить обучение персонала, ответственного за ее обслуживание.

## **4.3. Условия эксплуатации**

Программное решение "Стражник" предназначено для использования на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий. Ниже приведены условия эксплуатации данного программного продукта:

1. **Рабочая среда**: "Стражник" должен быть совместим с различными операционными системами, используемыми в рабочих станциях сотрудников МО и оборонных предприятий, включая Windows, Linux и macOS.
2. **Сетевое окружение**: Программное решение должно функционировать в сетевых средах с различными конфигурациями, включая локальные и распределенные сети, а также виртуальные среды.
3. **Безопасность**: "Стражник" должен соответствовать высоким стандартам безопасности информации и защите данных, установленным Министерством обороны Российской Федерации. Это включает в себя защиту от несанкционированного доступа, шифрование данных и обеспечение целостности информации.
4. **Отказоустойчивость**: Система должна быть спроектирована с учетом возможных сбоев и отказов оборудования, а также сетевых проблем, чтобы минимизировать простои и обеспечить непрерывную работу.
5. **Скорость и производительность**: Программное решение должно обеспечивать высокую скорость обработки событий и анализа данных для оперативного реагирования на угрозы безопасности.
6. **Обновления и поддержка**: Разработчики "Стражника" должны регулярно предоставлять обновления и техническую поддержку для обеспечения безопасности и эффективной работы программы.
7. **Интеграция**: Программное решение должно легко интегрироваться с существующими системами безопасности и инфраструктурой Министерства обороны Российской Федерации и оборонных предприятий.
8. **Документация и обучение**: Пользователям должны быть предоставлены подробная документация и обучение по установке, настройке и использованию программного решения "Стражник".

## **4.4. Требования к составу и параметрам технических средств**

Программное решение "Стражник" для системы централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий должно соответствовать следующим требованиям по составу и параметрам технических средств:

1. **Жесткие требования к безопасности**: Все компоненты программного решения должны соответствовать высоким стандартам безопасности, установленным Министерством обороны Российской Федерации. Это включает в себя механизмы шифрования данных, защиту от несанкционированного доступа и обеспечение целостности информации.
2. **Высокая производительность**: Технические средства, используемые для установки программного решения, должны обеспечивать достаточную производительность для оперативного мониторинга и анализа событий в реальном времени.
3. **Отказоустойчивость и надежность**: Все компоненты системы должны быть спроектированы с учетом возможных сбоев и отказов оборудования, чтобы минимизировать простои и обеспечить непрерывную работу даже в условиях экстремальных ситуаций.
4. **Совместимость и интеграция**: Технические средства должны легко интегрироваться с существующими информационными системами и инфраструктурой Министерства обороны Российской Федерации и оборонных предприятий.
5. **Масштабируемость**: Система должна быть способной масштабироваться в случае необходимости, чтобы обеспечить эффективное функционирование в условиях роста объема обрабатываемых данных и расширения сетевой инфраструктуры.
6. **Удобство обслуживания и администрирования**: Технические средства должны быть легкими в обслуживании и администрировании, чтобы минимизировать затраты на поддержку и обеспечить бесперебойную работу системы.
7. **Совместимость с различными операционными системами**: Программное решение должно быть совместимо с различными операционными системами, используемыми на рабочих станциях сотрудников Министерства обороны Российской Федерации и оборонных предприятий, включая Windows, Linux и macOS.

## **4.5. Требования к информационной и программной совместимости**

Для успешного развертывания программного решения "Стражник" в системе централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий необходимо обеспечить следующую информационную и программную совместимость:

1. **Совместимость с различными версиями операционных систем**: Программное решение должно работать без проблем на различных версиях операционных систем, используемых на рабочих станциях сотрудников, включая Windows, Linux и macOS.
2. **Интеграция с существующими информационными системами**: "Стражник" должен без проблем интегрироваться с уже существующими информационными системами и инфраструктурой Министерства обороны Российской Федерации и оборонных предприятий.
3. **Сетевая совместимость**: Программное решение должно функционировать в различных сетевых средах, включая локальные и распределенные сети, а также виртуальные среды, обеспечивая стабильное соединение и обмен данными.
4. **Совместимость с существующими программными решениями**: "Стражник" должен быть совместим с другими программными решениями, используемыми в секторе обороны, чтобы обеспечить эффективное взаимодействие и совместную работу.
5. **Обеспечение безопасности при интеграции**: при интеграции с другими системами необходимо обеспечить сохранность и конфиденциальность данных, а также защиту от возможных киберугроз и несанкционированного доступа.
6. **Обеспечение совместимости с будущими обновлениями и расширениями**: Разработанное программное решение должно быть гибким и легко адаптируемым для внедрения будущих обновлений и расширений, чтобы оно оставалось актуальным и функциональным на протяжении всего периода эксплуатации.

## **4.6. Требования к маркировке и упаковке**

Для программного решения "Стражник", предназначенного для системы централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны Российской Федерации (МО) и оборонных предприятий, следует предусмотреть следующие требования к маркировке и упаковке:

1. **Идентификация продукта**: Каждый экземпляр программного решения должен быть однозначно идентифицирован с помощью уникального серийного номера или другого идентификационного кода.
2. **Инструкции по установке и использованию**: В упаковке должны быть предоставлены подробные инструкции по установке, настройке и использованию программного решения на рабочих станциях.
3. **Требования к системным ресурсам**: на упаковке и в руководстве пользователя должны быть указаны минимальные и рекомендуемые требования к системным ресурсам (процессор, оперативная память, свободное место на диске и т. д.) для успешного функционирования программ

## **4.7. Требования к транспортированию и хранению**

1. **Защита от повреждений:** Упаковка должна обеспечивать достаточную защиту программного решения от механических повреждений и воздействия окружающей среды во время транспортировки и хранения.
2. **Устойчивость к условиям хранения:** Программное решение должно быть устойчиво к изменениям температуры, влажности и другим условиям хранения, характерным для условий транспортировки и хранения на оборонных объектах.
3. **Минимальные требования к хранению:** Упаковка должна содержать информацию о минимальных требованиях к условиям хранения, включая температурные и влажностные условия, для сохранения функциональности программного решения.
4. **Защита от несанкционированного доступа:** В случае длительного хранения, упаковка должна обеспечивать защиту от несанкционированного доступа к программным компонентам или конфиденциальной информации, включая меры шифрования или механизмы физической защиты.

## **4.8. Специальные требования**

Для разработки программного решения "Стражник", предназначенного для системы централизованного мониторинга событий на рабочих станциях сотрудников министерства обороны РФ (МО) и оборонных предприятий, необходимо учесть следующие специальные требования:

1. **Система журналирования:** решение должно обеспечивать полное и надежное журналирование всех событий и действий, происходящих в системе, с возможностью анализа и восстановления истории событий.
2. **Сетевая защита:** программное решение должно иметь встроенные механизмы защиты от сетевых атак и несанкционированного доступа, включая защиту от DDoS-атак, перехвата трафика и внедрения вредоносного ПО.
3. **Совместимость с системами безопасности:** "Стражник" должен быть совместим с существующими системами безопасности, используемыми в министерстве обороны и оборонных предприятиях, для обеспечения целостности и согласованности защитных мер.
4. **Автоматизированные оповещения:** решение должно обеспечивать возможность автоматической отправки оповещений о возникших событиях и инцидентах на рабочие станции сотрудников и ответственных лиц для оперативного реагирования на угрозы безопасности.
5. **Конфиденциальность данных:** "Стражник" должен обеспечивать высокий уровень конфиденциальности и защиты персональных данных сотрудников министерства обороны и оборонных предприятий в соответствии с требованиями законодательства о защите персональных данных.
6. **Резервное копирование и восстановление:** решение должно предоставлять средства для регулярного создания резервных копий данных и возможность быстрого восстановления системы в случае аварийных ситуаций или атак на информационную безопасность.
7. **Обучение и поддержка пользователей:** разработчики должны обеспечить поддержку пользователей в виде обучения персонала, консультаций по вопросам эксплуатации и технической поддержки для обеспечения эффективного использования программного решения.

# **ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ**

Для технического задания на разработку программного решения для "Стражник" - системы централизованного мониторинга событий на рабочих станциях сотрудников Министерства обороны РФ (МО) и оборонных предприятий, требуется следующая программная документация:

1. **Техническое описание:** документ должен содержать подробное описание архитектуры, функциональных возможностей и интерфейсов программного решения "Стражник".
2. **Инструкция по установке и настройке:** подробное руководство по установке, настройке и запуску программы, включая необходимые системные требования и последовательность действий.
3. **Руководство пользователя:** документ должен содержать информацию о работе с программным решением, его основных функциях, интерфейсе и способах взаимодействия с системой.
4. **Справочное руководство:** документация должна включать справочные материалы, объясняющие термины, понятия и процессы, связанные с использованием программы.
5. **Техническая поддержка:** документация должна содержать контактную информацию для получения технической поддержки, включая адреса электронной почты или номера телефонов специалистов по поддержке.

# **ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ**

Для составления технико-экономических показателей для технического задания на разработку программного решения "Стражник" необходимо провести анализ следующих аспектов:

1. **Затраты на разработку:** оценка трудозатрат и ресурсов, необходимых для создания программного решения, включая оплату труда разработчиков, закупку необходимого оборудования и программного обеспечения.
2. **Сроки разработки:** определение времени, необходимого для завершения разработки программного решения, с учетом всех этапов разработки и возможных задержек.
3. **Требуемое оборудование и программное обеспечение:** определение необходимого оборудования и программного обеспечения для развертывания и использования программного решения "Стражник".
4. **Ожидаемая экономическая выгода:** оценка ожидаемых экономических выгод от внедрения программного решения, включая уменьшение рисков информационной безопасности, повышение эффективности работы и сокращение затрат на обслуживание и поддержку.
5. **Оценка рентабельности проекта:** анализ ожидаемой рентабельности проекта с учетом затрат на разработку и ожидаемых экономических выгод.

# **СТАДИИ И ЭТАПЫ РАЗРАБОТКИ**

**Планирование и анализ требований:**

* 1. Определение функциональных и нефункциональных требований к программному решению "Стражник".
  2. Анализ требований заказчика и стейкхолдеров.

**Проектирование:**

* 1. Разработка архитектуры программного решения с учетом специальных требований.
  2. Проектирование интерфейса пользователя.
  3. Планирование системы журналирования и защиты данных.

**Разработка:**

* 1. Создание программного кода и функциональных модулей "Стражника" в соответствии с утвержденной архитектурой.
  2. Тестирование и отладка кода.

**Тестирование:**

* 1. Проведение модульного, интеграционного и системного тестирования.
  2. Верификация соответствия требованиям и исправление выявленных ошибок.

**Внедрение и сопровождение:**

* 1. Установка и настройка программного решения на рабочих станциях сотрудников Министерства обороны и оборонных предприятий.
  2. Обучение пользователей и их поддержка.
  3. Мониторинг и сопровождение работы системы, включая резервное копирование и восстановление данных.

# **ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ**

**Модульное тестирование:**

* 1. Разработчики должны провести модульное тестирование каждого компонента программного решения "Стражник" с целью проверки их работоспособности и соответствия функциональным требованиям.
  2. Результаты тестирования должны быть задокументированы, включая обнаруженные ошибки и способы их устранения.

**Интеграционное тестирование:**

* 1. После завершения разработки отдельных компонентов необходимо провести интеграционное тестирование для проверки их взаимодействия и совместимости.
  2. Тестирование должно охватывать все интерфейсы и взаимодействия между модулями.
  3. Результаты интеграционного тестирования также должны быть задокументированы.

**Системное тестирование:**

* 1. После интеграции всех компонентов программного решения следует провести системное тестирование для проверки его работы как единого целого.
  2. Это включает тестирование функциональности, производительности, безопасности и надежности системы в целом.
  3. Результаты системного тестирования должны быть задокументированы.

**Верификация соответствия требованиям:**

* 1. После завершения всех видов тестирования должна быть проведена верификация соответствия программного решения требованиям, описанным в разделе 4 данного технического задания.
  2. Все выявленные несоответствия должны быть устранены разработчиками до передачи решения на этап внедрения.

**Приемка и утверждение:**

* 1. После успешного прохождения всех видов тестирования и верификации соответствия требованиям заказчик должен провести процедуру приемки программного решения.
  2. Приемка включает в себя проверку выполнения всех функциональных и нефункциональных требований, а также согласованность с заявленными характеристиками.
  3. После успешной приемки заказчик должен утвердить программное решение для внедрения и эксплуатации.