УТВЕРЖДЕН

ПМ.02 Осуществление интеграции программных модулей

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

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

Техническое задание

Листов 16

2024

Содержание

[**1. ВВЕДЕНИЕ** 3](#_Toc165464441)

[**2. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ** 4](#_Toc165464442)

[**3. НАЗНАЧЕНИЕ РАЗРАБОТКИ** 5](#_Toc165464443)

[**4. ТРЕБОВАНИЯ К ПРОГРАММЕ ИЛИ ПРОГРАММНОМУ ИЗДЕЛИЮ** 6](#_Toc165464444)

[**4.1. Требования к функциональным характеристикам** 6](#_Toc165464445)

[**4.2. Требования к надежности** 6](#_Toc165464446)

[**4.3. Условия эксплуатации** 7](#_Toc165464447)

[**4.4. Требования к составу и параметрам технических средств** 8](#_Toc165464448)

[**4.5. Требования к информационной и программной совместимости** 8](#_Toc165464449)

[**4.6. Требования к маркировке и упаковке** 8](#_Toc165464450)

[**4.7. Требования к транспортированию и хранению** 9](#_Toc165464451)

[**4.8. Специальные требования** 9](#_Toc165464452)

[**5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ** 11](#_Toc165464453)

[**6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ** 12](#_Toc165464454)

[**7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ** 13](#_Toc165464455)

[**8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ** 15](#_Toc165464456)

# **1. ВВЕДЕНИЕ**

Система "Стражник" представляет собой важное средство обеспечения информационной безопасности для министерства обороны РФ и оборонных предприятий. Ее основная цель – обнаруживать и реагировать на потенциальные угрозы в реальном времени, обеспечивая надежную защиту конфиденциальных данных и соблюдение стандартов безопасности. Система включает в себя разнообразные инструменты мониторинга, обработки и аудита событий на рабочих станциях пользователей, а также средства визуализации данных и механизмы оповещения для оперативного реагирования службы безопасности. "Стражник" способствует эффективной работе службы безопасности и повышению уровня защиты информации от внешних и внутренних угроз.

# **2. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ**

Основанием для разработки системы "Стражник" является необходимость обеспечения информационной безопасности министерства обороны РФ и оборонных предприятий. С учетом угроз кибербезопасности, важно иметь систему централизованного мониторинга событий на рабочих станциях сотрудников, которая позволит оперативно выявлять и реагировать на потенциальные угрозы.

Система "Стражник" разрабатывается для обеспечения надежной защиты конфиденциальных данных, соблюдения стандартов безопасности и обеспечения условий мандатного доступа к данным пользователей. Включение инструментов мониторинга, обработки и аудита событий на ПК пользователей, а также средств визуализации данных и механизмов оповещения службы ИБ о нарушениях протоколов безопасности, делает систему эффективным инструментом для обеспечения безопасности информации и оперативного реагирования на угрозы.

# **3. НАЗНАЧЕНИЕ РАЗРАБОТКИ**

Назначение разработки системы "Стражник" заключается в обеспечении информационной безопасности министерства обороны РФ и оборонных предприятий путем создания централизованной системы мониторинга событий на рабочих станциях сотрудников. Система предназначена для обнаружения возможных угроз информационной безопасности в реальном времени, оперативного реагирования на них, отправки уведомлений службе безопасности и обеспечения соблюдения условий мандатного доступа к данным пользователей.

Ключевые задачи системы "Стражник" включают в себя:

1. Мониторинг событий на персональных компьютерах пользователей для выявления потенциальных угроз.

2. Обработка и аудит событий с целью анализа и классификации возможных угроз.

3. Визуализация данных для службы информационной безопасности для обеспечения понимания текущей ситуации.

4. Механизмы оповещения службы ИБ о событиях, нарушающих протоколы безопасности, для оперативного реагирования.

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

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

Требования к функциональным характеристикам программы "Стражник" включают следующие пункты:

1. Мониторинг событий на персональных компьютерах пользователей в режиме реального времени.

2. Обнаружение и классификация потенциальных угроз информационной безопасности.

3. Оперативное реагирование на угрозы и принятие соответствующих мер безопасности.

4. Отправка уведомлений службе безопасности о выявленных событиях.

5. Соблюдение условий мандатного доступа к данным пользователей.

6. Инструменты для обработки и аудита событий на ПК пользователей.

7. Средства визуализации данных для службы информационной безопасности.

8. Механизмы оповещения службы ИБ о событиях, нарушающих протоколы безопасности.

## **4.2. Требования к надежности**

Требования к надежности программы "Стражник" включают:

1. Высокую стабильность работы системы централизованного мониторинга событий.

2. Отказоустойчивость и возможность быстрого восстановления после сбоев.

3. Защиту от несанкционированного доступа к данным и функционалу программы.

4. Гарантию сохранения конфиденциальности информации, обрабатываемой программой.

5. Обеспечение целостности данных и их защиту от порчи или утраты.

6. Регулярное резервное копирование данных для предотвращения потери информации.

7. Обеспечение соответствия требованиям безопасности и конфиденциальности при обработке данных пользователей.

## **4.3. Условия эксплуатации**

Для обеспечения надежной работы программы "Стражник" в условиях эксплуатации на рабочих станциях сотрудников Министерства обороны РФ и оборонных предприятий следует учитывать следующие аспекты:

1. Система должна быть способна работать в режиме реального времени для оперативного выявления угроз информационной безопасности.

2. Необходимо обеспечить высокую производительность системы, чтобы она могла эффективно обрабатывать большие объемы данных.

3. Важно уделить особое внимание защите конфиденциальности данных пользователей и соблюдению условий мандатного доступа к информации.

4. Система должна быть отказоустойчивой и иметь механизмы быстрого восстановления после сбоев.

5. Предусмотреть механизмы резервного копирования данных для обеспечения их целостности и возможности восстановления.

6. Обеспечить защиту от несанкционированного доступа к данным и функционалу программы.

7. Гарантировать соответствие требованиям безопасности и конфиденциальности при обработке данных пользователей.

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

Для разработки программного решения "Стражник" для организации пропускного режима на объекте КИИ, необходимо определить требования к составу и параметрам технических средств. Ниже приведены основные требования к техническим средствам для данного проекта:

1. Процессор: не ниже Pentium 3 – 800 MHz;
2. Оперативная память: не менее 128 Mb;
3. Место на жестком диске: не менее 120 Mb;
4. ОС: Windows 8 – Windows 10;
5. Интернет соединение: не ниже 64 Кб/сек (опционально);
6. Монитор: SVGA монитор;
7. Другие требования: сетевая карта, клавиатура, манипулятор мышь.

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

Программный продукт должны быть написана на языке С#. Системные программные средства, используемые программой, должны быть представлены лицензионной локализованной версией операционной системы Windows 7, Windows 8, Windows 10. Программный продукт создается с использованием инструментального средства разработки приложений MS Project, Visio.

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

Ввиду специфики системы "Стражник" и ее назначения для Министерства обороны РФ и оборонных предприятий, требования к маркировке и упаковке должны соответствовать строгим стандартам безопасности и конфиденциальности.

**Маркировка:**

* Минимализм: Внешняя маркировка должна быть минимальной и не раскрывать содержимое упаковки.
* Уникальные идентификаторы: Каждая упаковка должна иметь уникальный идентификатор для отслеживания и инвентаризации.
* Классификация информации: Уровень секретности информации, содержащейся в системе, должен быть указан на упаковке в соответствии с действующими нормативными документами.
* Специальные отметки: В случае необходимости, упаковка должна иметь специальные отметки, указывающие на особые условия хранения или транспортировки.

**Упаковка:**

* Защита от несанкционированного доступа: Упаковка должна обеспечивать надежную защиту от несанкционированного доступа к содержимому. Это может включать использование пломб, специальных замков или других средств защиты.
* Защита от повреждений: Упаковка должна защищать содержимое от повреждений во время транспортировки и хранения.
* Устойчивость к внешним воздействиям: Упаковка должна быть устойчивой к воздействию влаги, температурных перепадов и других внешних факторов.
* Экологичность: Материалы упаковки должны соответствовать экологическим стандартам и быть пригодными для утилизации.

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

Специальных требований не предъявляется.

## **4.8. Специальные требования**

Специальные требования не предъявляются.

# 

# **5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ**

Состав программной документации должен включать в себя:

1. Техническое задание
2. Архитектурная документация
3. Инструкция по установке и настройке
4. Руководство пользователя
5. Тестовая документация
6. Лицензионная документация
7. Документация по безопасности

# **6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ**

Ориентировочная экономическая эффективность не рассчитывается. Аналогия не проводится ввиду уникальности предъявляемых требований к разработке.

# **7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ**

Разработка должна быть проведена в три стадии:

1) Техническое задание;

2) Технический (и рабочий) проекты;

3) Внедрение.

На стадии «Техническое задание» должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания. На стадии «Технический (и рабочий) проект» должны быть выполнены перечисленные ниже этапы работ:

1) Разработка программы;

2) Разработка программной документации;

3) Испытания программы. На стадии «Внедрение» должен быть выполнен этап разработки «Подготовка и передача программы».

Содержание работы по этапам. На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

1) Постановка задачи;

2) Определение и уточнение требований к техническим средствам;

3) Определение требований к программе;

4) Определение стадий, этапов и сроков разработки программы и документации на нее;

5) Согласование и утверждение технического задания. На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы. На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями ГОСТ 19.102- 77. На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:

1) Разработка, согласование и утверждение порядка и методики испытаний;

2) Проведение приемо-сдаточных испытаний;

3) Корректировка программы и программной документации по результатам испытаний. На этапе подготовки и передачи программы должна быть выполнена работа по подготовке и передаче программы и программной документации в эксплуатацию на объектах заказчика.

# **8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ**

1. Подготовка к контролю и приемке:

* + Перед началом контроля необходимо убедиться в готовности всех компонентов системы «Стражник» к работе.
  + Подготовить необходимое оборудование для проведения контроля и приемки.

2. Проведение контроля и приемки:

* + Проверить работоспособность инструментов мониторинга, обработки и аудита событий на ПК пользователей.
  + Убедиться в корректной работе средств визуализации данных для службы ИБ.
  + Проверить механизмы оповещения службы ИБ о нарушениях протоколов безопасности.
  + Провести тестирование реакции системы на возможные угрозы информационной безопасности.
  + Проверить отправку уведомлений службе безопасности и соблюдение условий мандатного доступа к данным пользователей.

3. Оценка результатов контроля:

* Оценить эффективность работы системы «Стражник» в выявлении угроз ИБ и оперативной реакции на них.
* Проверить соответствие функциональных возможностей системы заявленным требованиям.
* Оценить качество визуализации данных и удобство работы с системой для службы ИБ.

4. Фиксация результатов и подписание акта приемки:

* Зафиксировать результаты контроля и приемки в специальном отчете.
* Подписать акт приемки системы «Стражник» представителями Министерства обороны РФ и оборонных предприятий.
* В случае выявления недочетов или несоответствий, составить план мероприятий по их устранению.