УТВЕРЖДАЮ

»

_____

М.П.

«____» _____2024 г.

УТВЕРЖДАЮ

_____

М.П.

«____» _____2024 г.

РАЗРАБОТКА ПРОГРАММНОЙ ДОКУМЕНТАЦИИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Разработка средства удаленного доступа к отечественным ОС с использованием аппаратной криптографии через PKCS#11

Москва 2024

СОДЕРЖАНИЕ

1 Общие сведения

1.1 Наименование программы

Наименование программы – «_____».

1.2 Краткая характеристика области применения

Данная программа предназначена для обеспечения безопасного удаленного доступа к отечественным операционным системам с использованием аппаратной криптографии через стандарт PKCS#11.

2. Основания для разработки

Основанием для разработки является Договор _____ от _____ (дата). Договор утвержден Директором _____, именуемым в дальнейшем Заказчиком, и _____, именуемым в дальнейшем исполнителем, _____ (дата).

Согласно Договору, Исполнитель обязан разработать и установить систему «_____» на оборудовании Заказчика не позднее _____ (дата), предоставить исходные коды и документацию к разработанной системе не позднее _____ (дата).

Наименование темы разработки – «Разработка средства удаленного доступа к отечественным ОС с использованием аппаратной криптографии через PKCS#11».

Условное обозначение темы разработки (шифр темы) – «_____».

3 Назначение разработки

Программа будет использоваться в МГТУ им. Н.Э. Баумана пользователями (студенты, сотрудники).

3.1 Функциональное назначение

Для посетителя (студент, сотрудник) МГТУ им. Н.Э. Баумана программа предоставляет возможность безопасного удаленного доступа к отечественным операционным системам с использованием аппаратной криптографии через стандарт PKCS#11.

3.2 Эксплуатационное назначение

Программа должна эксплуатироваться в МГТУ им. Н.Э. Баумана. В соответствии с предоставленными сертификатами пользователям предоставляется удаленный доступ к выделенным отечественным операционным системам на территории МГТУ им. Н.Э. Баумана с установленными правами на выполнение административных задач, доступ к защищенным данным и ресурсам сети университета, а также возможность управления конфигурациями и настройками систем в соответствии с их должностными обязанностями и уровнем доступа.

4 Требования к программе или программному изделию

4.1 Требования к функциональным характеристикам

4.1.1 Требования к составу выполняемых функций

- **Аутентификация и авторизация.** Система должна обеспечивать безопасную аутентификацию пользователей перед предоставлением доступа к отечественным операционным системам. Для этого необходимо использовать аппаратную криптографию через PKCS#11 для защиты ключевой информации и обеспечения безопасного доступа.
- **Шифрование данных.** Средство удаленного доступа должно обеспечивать шифрование данных, передаваемых между пользователем и отечественными операционными системами, с использованием аппаратной криптографии по стандарту PKCS#11. Это гарантирует конфиденциальность и целостность передаваемой информации.
- **Управление ключами.** Система должна обеспечивать безопасное управление ключами шифрования и аутентификации через стандарт PKCS#11. Это включает генерацию, хранение, использование и уничтожение ключей с помощью аппаратных средств криптографии.

- **Целостность и подлинность.** Средство удаленного доступа должно гарантировать целостность и подлинность передаваемых данных путем использования цифровых подписей и проверки целостности данных с использованием аппаратной криптографии.

- **Отслеживание и журналирование.** Система должна обеспечивать возможность отслеживания действий пользователей при доступе к отечественным операционным системам, а также ведение журналов событий для обеспечения безопасности и контроля доступа.
- **Совместимость и масштабируемость.** Разработанное средство удаленного доступа должно быть совместимо с отечественными операционными системами и обладать возможностью масштабирования для работы в различных сетевых средах и условиях.
- **Обновление и поддержка.** Система должна иметь механизмы для обновления программного обеспечения, поддержки стандартов безопасности и регулярного аудита для обеспечения надежной работы и защиты от уязвимостей.

4.1.2 Требования к организации входных и выходных данных

- Входные данные должны быть защищены аппаратной криптографией по стандарту PKCS#11 для обеспечения конфиденциальности и целостности.
- Выходные данные должны быть шифрованы с использованием аппаратной криптографии через PKCS#11 для обеспечения безопасной передачи информации.
- Данные, передаваемые между пользователем и отечественными операционными системами, должны быть подписаны и проверены на целостность с применением аппаратной криптографии.
- Все операции с данными должны быть журналированы для обеспечения отслеживаемости и контроля доступа к системе удаленного доступа.
- Система должна обеспечивать возможность управления ключами шифрования и аутентификации через стандарт PKCS#11 для обеспечения безопасности и надежности работы.

4.1.3 Требования к временным характеристикам

- Средство удаленного доступа к отечественным операционным системам должно обеспечивать мгновенное установление безопасного соединения с использованием аппаратной криптографии через PKCS#11.
- Время отклика на запросы пользователя не должно превышать установленный порог в течение 500 миллисекунд для обеспечения эффективного взаимодействия.
- Передача данных и выполнение операций шифрования/дешифрования должны осуществляться с минимальной задержкой, не превышающей 100 миллисекунд, для обеспечения быстрой реакции на запросы пользователя.
- Система должна обеспечивать моментальное отключение доступа при обнаружении подозрительной активности или нарушений безопасности для предотвращения утечки данных и несанкционированного доступа.

4.2 Требования к надежности

Вероятность безотказной работы системы должна составлять не менее 99.99% при условии исправности сети.

4.2.1 Требования к обеспечению надежного (устойчивого) функционирования программы

Программа должна обеспечивать надежное и устойчивое функционирование при работе с аппаратной криптографией через PKCS#11, минимизируя возможность сбоев и ошибок.

4.2.2 Время восстановления после отказа

Время восстановления программы после возможного отказа должно быть минимальным, обеспечивая быстрое восстановление работы для минимизации простоев и негативного влияния на процессы доступа к операционным системам.

4.2.3 Отказы из-за некорректных действий

Программа должна предотвращать отказы, вызванные некорректными действиями пользователей или системных агентов, обеспечивая защиту от ошибок и несанкционированных операций при удаленном доступе к отечественным операционным системам через PKCS#11

4.3 Условия эксплуатации

- Разработка средства удаленного доступа к отечественным операционным системам с использованием аппаратной криптографии через PKCS#11 должна обеспечивать стабильную работу при различных нагрузках и условиях сетевой инфраструктуры.
- Система должна быть легко масштабируемой и готовой к интеграции с другими информационными технологиями, обеспечивая высокую производительность и надежность в различных сценариях использования.

- Пользовательский интерфейс должен быть интуитивно понятным и удобным для конечных пользователей, минимизируя необходимость специальной подготовки и обучения для работы с системой удаленного доступа.
- Обеспечение безопасности передачи данных и аутентификации пользователей должно быть приоритетом, гарантируя конфиденциальность и защиту информации при использовании средства удаленного доступа через PKCS#11.

4.4 Требования к составу и параметрам технических средств

- Система должна поддерживать аппаратные средства криптографии, совместимые с протоколом PKCS#11, обеспечивая безопасное хранение ключей и операции шифрования на уровне устройства.
- Технические средства должны обладать высокой производительностью и надежностью, гарантируя оперативный доступ к отечественным операционным системам через удаленное подключение.
- Компоненты системы должны быть совместимы с различными версиями отечественных ОС, обеспечивая стабильную работу и совместимость с широким спектром конфигураций и настроек.
- Параметры технических средств должны соответствовать требованиям безопасности и производительности, обеспечивая эффективное функционирование системы удаленного доступа через PKCS#11.

4.5 Требования к информационной и программной совместимости

Система должна быть совместима с существующими информационными системами и программным обеспечением, используемым на отечественных операционных системах.

4.6 Требование к маркировке и упаковке

Продукция должна быть четко маркирована с указанием модели, серийного номера и других идентификационных данных. Упаковка должна обеспечивать защиту от повреждений во время транспортировки.

4.7 Требования к транспортированию и хранению

При транспортировке необходимо обеспечить защиту от физических и кибератак. Хранение должно осуществляться в соответствии с рекомендациями производителя для обеспечения долговечности и безопасности устройств.

4.8 Специальные требования

Система должна иметь возможность автоматической конфигурации и обновления для обеспечения безопасности и стабильной работы при использовании аппаратной криптографии через PKCS#11.

5 Требования к программной документации

Предварительный состав программной документации:

- техническое задание (включает описание применения);
- программа и методика испытаний;
- руководство системного программиста;
- руководство оператора;
- руководство программиста;
- ведомость эксплуатационных документов;
- формуляр.

6 Технико-экономические показатели

- Анализ затрат на разработку средства удаленного доступа к отечественным ОС с использованием аппаратной криптографии через PKCS#11.
- Прогноз ожидаемой экономии благодаря повышению безопасности и эффективности системы.
- Оценка возвратности инвестиций и ожидаемых финансовых результатов от внедрения нового средства удаленного доступа.
- Сравнительный анализ существующих решений на рынке и прогноз конкурентоспособности разрабатываемого продукта.
- Оценка рисков и возможных финансовых потерь в процессе разработки и внедрения новой системы удаленного доступа.

7 Стадии и этапы разработки

Разработка должна быть проведена в три стадии:

- техническое задание;

- технический (и рабочий) проекты;
- 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:

- разработка программы;
- разработка программной документации;
- испытания программы.

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

- Содержание работ по этапам:

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

- постановка задачи;
- определение и уточнение требований к техническим средствам;
- определение требований к программе;
- определение стадий, этапов и сроков разработки программы и документации на нее;
- 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 19.101-77.

На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:

- разработка, согласование и утверждение порядка и методики испытаний;
- проведение приемо-сдаточных испытаний;
- 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

Приемосдаточные испытания программы должны проводиться согласно разработанной исполнителем и согласованной заказчиком «Программы и методики испытаний».

Ход проведения приемо-сдаточных испытаний заказчик и исполнитель документируют в протоколе испытаний.

На основании протокола испытаний исполнитель совместно с заказчиком подписывают акт приемки-сдачи программы в эксплуатацию.

Список используемой литературы

1. ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению. 1978. Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=155153

2. ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения. М.: Издательство стандартов, 1987. – 17 с.