УДК 004

Насифуллина Э.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ СООТВЕТСТВИЯ СУЩЕСТВУЮЩИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТРЕБОВАНИЯМ ГОСТ ПРИ СОЗДАНИИ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Аннотация. В данной статье проводится анализ соответствия современных средств защиты информации требованиям государственного стандарта, регулирующих создание автоматизированных систем в защищенном исполнении. Целью исследования является выявление степени готовности рынка средств защиты информации к обеспечению необходимого уровня защиты информации в автоматизированных систем, создаваемых в соответствии с требованиями государственного стандарта.

Ключевые слова: средства защиты информации, ГОСТ, автоматизированные системы, сертификация, ФСТЭК.

В настоящее время проблема соответствия СЗИ требованиям ГОСТ Р 51583-2014 остается крайне актуальной [8]. Развитие технологий приводит к появлению новых угроз, что делает важным постоянное обновление механизмов защиты информации. Многие организации сталкиваются с трудностями при выборе сертифицированных средств защиты, а также с необходимостью интеграции разнородных систем безопасности. Анализируя ГОСТ Р 51583-2014, мы видим, что стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством уже определены, а заказчиком определяются требования по их защите, содержание и порядок выполнения работ на соответствующих стадиях и этапах создания в защищенном исполнении [1]. Иными словами, стандарт устанавливает базовые принципы, требования и рекомендации по организации процесса создания и функционирования защищенных АС.

Таким образом, ГОСТ Р 51583-2014 определяет общий порядок создания АС в защищенном исполнении, охватывая весь жизненный цикл системы: от этапа предпроектных исследований до ввода в эксплуатацию и последующего вывода из нее. Это можно установить по перечню, в котором содержатся отсылочные нормы, регулирующие конкретные этапы. Так, на этапе предпроектных исследований необходимо выполнить ряд ключевых шагов, среди которых:

- определение целей защиты информации;
- формирование перечня актуальных угроз;
- проведение анализа рисков;
- разработка модели угроз и модели нарушителя.

На основе этих данных формируются требования по защите информации, включающие в себя требования конфиденциальности, целостности и доступности информации. Технический проект должен детально описывать архитектуру системы защиты, состав и характеристики СЗИ, а также методы их интеграции и настройки. Процесс внедрения СЗИ должен включать в себя аттестацию, которая подтверждает соответствие внедренных средств установленным требованиям по безопасности информации. После ввода в эксплуатацию АС в защищенном исполнении требуется обеспечить постоянное сопровождение системы защиты: ее актуализацию, регулярный мониторинг и анализ инцидентов информационной безопасности.

Для детального анализа соответствия существующих средств защиты информации требованиям ГОСТ при создании АС в защищенном исполнении проанализируем и оценим, насколько современные средства защиты информации соответствуют требованиям ГОСТ Р 51583-2014, выявим возможные расхождения и несоответствия различных категорий СЗИ предъявляемым требованиям.

В современных межсетевых экранах (МСЭ), например «Страж NT» (версия 4.0) компании ООО «РУБИНТЕХ», который может применяться

для комплексной защиты информационных ресурсов от несанкционированного доступа и фильтрацию трафика при работе в одно- и многопользовательских автоматизированных системах (АС) [2] и «Континент» (разработчик – компания «Код Безопасности»)[3] сертифицирован ФСТЭК России и соответствует требованиям ГОСТ в части фильтрации трафика, защиты от несанкционированного доступа и обеспечения безопасных соединений, несмотря на соответствие ключевым требованиям, возможны сложности в интеграции с определенными зарубежными решениями, а также они нуждаются в дополнительной настройке под специфические политики безопасности конкретных организаций.

В свою очередь, антивирусные решения Kaspersky Endpoint Security и Dr.Web соответствуют требованиям по обнаружению и нейтрализации вредоносного кода [4], однако при их применении в крупных автоматизированных системах важно учитывать необходимость централизованного управления, что может потребовать дополнительных программных средств, таких как «Касперский Центр Управления Безопасностью». Кроме того, обновление сигнатурных баз и механизмов поведенческого анализа должно быть оперативным, чтобы соответствовать современным требованиям защиты информации, установленным в ГОСТ Р 51583-2014.

Система обнаружения вторжений «Рубикон» (разработчик – компания «НПО Эшелон») [5], соответствует требованиям ГОСТ, обеспечивая мониторинг сетевого трафика, выявление аномалий и автоматизированное реагирование на инциденты. Однако их эффективность зависит от своевременной настройки политик безопасности, анализа инцидентов и актуальности баз данных угроз.

Современные отечественные средства криптографической защиты информации ViPNet CSP (разработчик – «ИнфоТеКС») [6], а также «КриптоПро CSP» полностью соответствуют сертификационным требованиям ФСБ России. Более того, ViPNet CSP обладает дополнительными возможностями по обеспечению защищенного соединения в распределенных сетях и поддерживает современные алгоритмы шифрования. Однако, несмотря на соответствие ключевым требованиям, здесь также могут возникать сложности с интеграцией в инфраструктуру, где используются зарубежные решения или устаревшие системы.

DLP-системы, такие как SearchInform и InfoWatch, а также «Стахановец» [7], соответствуют требованиям ГОСТ, контролируют каналы передачи данных и предотвращают утечки информации. При этом «Стахановец» предлагает расширенные возможности аналитики пользовательской активности, что позволяет не только предотвращать утечки, но и выявлять потенциальные внутренние угрозы. Однако для эффективного применения всех возможностей этих систем требуется детальная настройка под бизнес-процессы организации.

Таким образом, современные средства защиты информации в целом соответствуют требованиям ГОСТ Р 51583-2014. Однако на практике

могут возникать определенные сложности, связанные с проведением дополнительных настроек, их интеграцией в существующие программные и аппаратные решения, а также прохождения процедур аттестации, что требует комплексного подхода на всех этапах жизненного цикла защищенной автоматизированной системы.

Список использованных источников:

1. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 23.03.2025).

2. Страж NT 4.0. URL: https://guardnt.ru/gnt_40.html (дата обращения: 24.03.2025).

3. Решения Код безопасности. URL: https://kontinent-ipc.ru/ (дата обращения: 24.03.2025).

4. Kaspersky Endpoint Security для Windows | Лаборатория Касперского URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-windows (дата обращения: 28.03.2025).

5. ПАК «Рубикон». URL: https://npo-echelon.ru/production/65/11342 (дата обращения: 28.03.2025)

6. Сертифицированный криптопровайдер ViPNet CSP 4 | ИнфоТеКС. URL: https://infotecs.ru/products/vipnet-csp/ (дата обращения: 28.03.2025).

7. Предотвращение утечек информации – DLP-система | Стахановец URL: https://stakhanovets.ru/dlp/ (дата обращения: 28.03.2025).

8. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

Nasifullina E.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ANALYSIS OF THE COMPLIANCE OF EXISTING INFORMATION SECURITY TOOLS WITH THE REQUIREMENTS OF GOST WHEN CREATING AUTOMATED SYSTEMS IN A SECURE DESIGN

Abstract. This article analyzes the compliance of modern information security tools with the requirements of the state stardart governing the creation of automated systems in a secure design. The purpose of the study is to identify the degree of readiness of the information security market to ensure the

necessary level of information protection in automated systems created in accordance with the requirements of the state standard.

Keywords: information security tools, GOST, automated systems, information security, FSTEC.