УДК 004.056

А.Д.Михалева[1], С.П.Серёдкин[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

КОНЦЕПЦИЯ НУЛЕВОГО ДОВЕРИЯ КАК МОДЕЛЬ БЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация. В статье рассматривается концепция нулевого доверия как современная модель обеспечения безопасности государственных информационных систем. Рассматриваются принципы и состав данного подхода к обеспечению защиты информации, а также преимущества применения принципа нулевого доверия в современные условия. Приводятся статистика данных о текущих угрозах, направленных на государственный сектор. Делается вывод о необходимости перехода на архитектуру нулевого доверия для повышения устойчивости функционирования государственных информационных систем.

Ключевые слова: *информационная безопасность, государственная система, нулевое доверие, концепция, архитектура безопасности, защита данных.*

A.D.Mihaleva[1], S.P.Seredkin[1]

[1]Irkutsk State Transport University, Irkutsk, the Russian Federation

ZERO TRUST CONCEPT AS A SECURITY MODEL FOR THE STATE INFORMATION SYSTEM

Abstract. *The article considers the concept of zero trust as a modern model for ensuring the security of state information systems. The principles and composition of this approach to information security are considered, as well as the advantages of applying the principle of zero trust in modern conditions. The statistics of data on current threats aimed at the public sector are presented. It is concluded that it is necessary to switch to a zero-trust architecture in order to increase the stability of the functioning of state information systems.*

Keywords: *information security, government system, zero trust, concept, security architecture, data protection.*

Введение. В условиях стремительного роста цифровизации общества и экономики обеспечение безопасности информации в государственных системах приобретает ключевое значение. Государственные информационные системы подвергаются атакам, целью которых является компрометация данных, саботаж инфраструктуры и шпионаж. Традиционные подходы к кибербезопасности, основывающиеся на периметральной защите, утрачивают эффективность из-за увеличения сложности IT-инфраструктур и расширения количества точек доступа. В ответ на потребность пересмотра подхода к построению архитектуры появилась концепция нулевого доверия (Zero Trust), изложенная в стандарте Национального института стандартов и технологий (NIST) [1].

Концепция «полного недоверия» или модель «нулевого доверия», как обновление классического подхода к защите сетевого периметра была впервые предложена аналитиком Forrester Research Джоном Киндервагом (John Kindervag) в 2010 году и получила название Zero Trust (ZT).

Первое использование подхода Zero Trust в России началось ещё в 2020 году, но тогда это были больше теоретические рассуждения, чем попытки практического применения.

В период пандемии применение концепции Zero Trust и Zero Trust Network Access (сетевой доступ с нулевым доверием) позволило успешно противостоять угрозам и выстроить безопасную инфраструктуру в рамках распределённых информационных структур.

В 2021 году на онлайн-конференции AM Live «Сетевой доступ с нулевым доверием» эксперты обсудили принципы Zero Trust Network Access, его архитектуру, технические особенности, основные моменты или проблемы, возникающие при внедрении этой модели, а также тенденции по развитию и распространению решений, её реализующих [7].

Концепция нулевого доверия представляет собой модель безопасности, в рамках которой доступ к ресурсам предоставляется только после строгой проверки идентичности и соответствия запрашиваемых прав минимально необходимым требованиям. Все взаимодействия требуют проверки, независимо от местоположения пользователя или устройства. Основной принцип – "никому не доверяй, всегда проверяй". Целью такой модели безопасности является предотвращение несанкционированного доступа и максимально возможная детализация контроля доступа.

Проблематика. По статистике, опубликованной компанией Positive Technologies, в государственном секторе главными угрозами остаются вредоносное ПО (56% атак), социальная инженерия (25%) и эксплуатация уязвимостей в ПО (15%). Данные представлены на рис. 1.

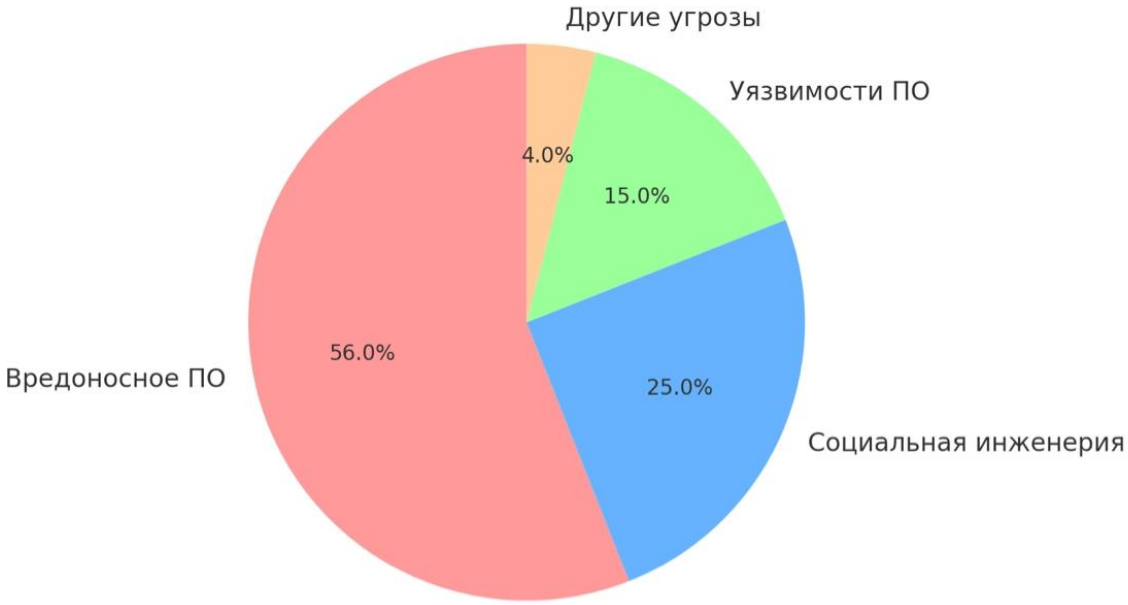

Рис.1. Статистика киберугроз в государственном секторе в 2024

Злоумышленники нацелены на кражу данных, вымогательство и нарушение работы критически важных систем, используя сложные инструменты и методы. Тренды 2024 года включают снижение популярности шифровальщиков и рост атак через фишинг и двойное вымогательство [11].

Для государственных органов утечка информации или нарушение ее целостности могут привести к серьезным последствиям: подрыву национальной безопасности, экономическим потерям и кризису доверия граждан. Использование концепции нулевого доверия позволяет значительно повысить устойчивость государственных информационных систем к современным угрозам и обеспечить защиту данных в условиях увеличивающегося числа киберугроз.

Согласно исследованию Microsoft, проведенному в 2021 году, 96% респондентов подтвердили, что поход нулевого доверия является критически важным для успеха работы их организации [12].

В настоящее время данная концепция развита гораздо больше и ее реализацию в своих решениях предлагают отечественные производители «UserGate», «Код Безопасности» и «ИнфоТеКС».

1. Принципы и компоненты концепции нулевого доверия

Не доверять никому по умолчанию.

Каждый пользователь и каждое устройство должны подтверждать свою подлинность, независимо от того, находятся они внутри сети или вне её. Доверие не предоставляется автоматически. Реализация доступа представлена на рис. 2.

Минимальный доступ к данным.

Доступ к информации и ресурсам предоставляется только в том объёме, который необходим для выполнения конкретных задач. Принцип минимизации привилегий помогает снизить риски.

Постоянный мониторинг и проверка.

Все действия пользователей и устройств должны постоянно отслеживаться и анализироваться, чтобы своевременно выявлять подозрительную активность или аномалии.

Сегментация сети.

Система должна быть разделена на изолированные зоны, чтобы минимизировать возможные последствия проникновения злоумышленников в одну из частей сети.

Многоуровневая защита.

Данные и ресурсы защищаются на каждом уровне: от пользователя и устройства до сети и приложений. Это обеспечивает защиту даже в случае взлома одной из систем.

Предположение о нарушении безопасности.

Подход предполагает, что угроза может существовать уже сейчас, поэтому каждая потенциальная уязвимость рассматривается как реальный риск и заранее принимаются меры для его предотвращения [3].

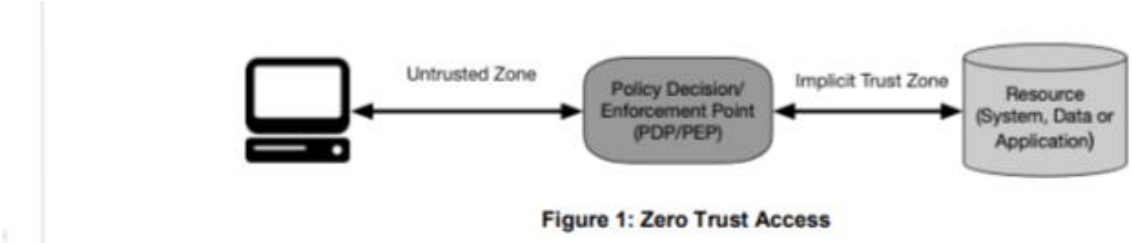

Figure 1: Zero Trust Access

Рис.2. Реализация доступа с нулевым доверием

Основа концепции изложена в NIST Special Publication 800-207 и может быть использована для внедрения модели доступа с нулевым доверием в организациях. В данном стандарте также представлена абстрактная логическая модель архитектуры Zero Trust, представленная на рис. 3.

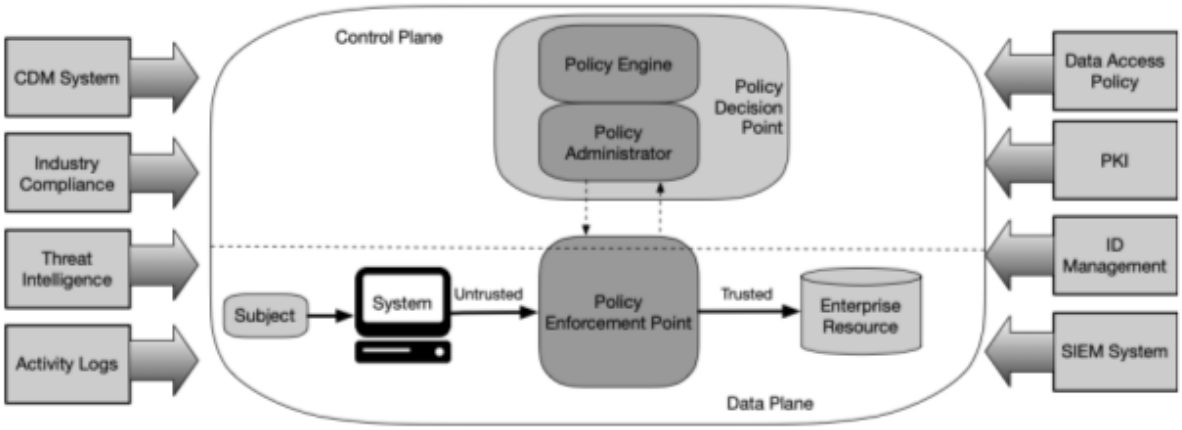

Figure 2: Core Zero Trust Logical Components

Рис 3. Основные логические компоненты модели нулевого доверия

Основными элементами данной модели являются:

– механизм политик (Policy Engine, PE) – ядро реализации ZTA, компоненты, на которых производится оценка возможности доступа в рамках запросов, обычно основанная на данных из различных источников (систем и журналов мониторинга, систем выявления угроз на конечных точках и др.);

– администратор политики (Policy Administrator, PA) – компонент, выполняющий политики, заданные на PE и обеспечивающие установление, поддержание и прекращение сеансов доступа через плоскость управления (набор каналов между всеми элементами модели);

– точка применения политик (Policy Enforcement Point, PEP) – компонент, с которым взаимодействуют субъекты, осуществляющие запросы доступа к информационным активам, выполняющий сбор сведений о субъектах доступа и их проверку по политикам, полученным от PA;

– информационные потоки (Policy Information Points, PIPs) – потоки, не являющиеся основными функциональными компонентами модели нулевого доверия, но используемые для поддержки функционирования PE за счёт предоставления данных для принятия решений по запросам доступа.

2. Необходимость внедрения принципа нулевого доверия в органах государственной власти

Угрозы кибербезопасности для государственного сектора

Государственные органы являются мишенью для множества кибератак, включая фишинговые кампании, взломы с использованием уязвимостей, атаки с применением программ-вымогателей и распространение дезинформации. Рост числа удаленных сотрудников и расширение использования облачных технологий увеличивают сложность защиты IT-систем [11].

Примеры инцидентов

Примером значительного инцидента является взлом системы SolarWinds, который затронул многочисленные государственные учреждения США. Атака продемонстрировала необходимость изменения подхода к кибербезопасности и усиления контроля над внутренними и внешними точками доступа. Также взломы систем или компрометация данных государственных учреждений подчеркивают необходимость перехода на более строгие подходы управления информационной безопасностью, включая Zero Trust [6].

3. Этапы внедрения концепции нулевого доверия

Оценка текущего состояния IT-систем

Первым шагом является аудит существующей инфраструктуры, включающий оценку уязвимостей, инвентаризацию информационных активов и устройств, а также анализ текущих политик безопасности. Это позволяет определить слабые места и приоритеты для внедрения концепции Zero Trust.

Разработка политики доступа

На основе принципов минимизации привилегий разрабатывается политика доступа, которая ограничивает права пользователей и устройств в соответствии с их функциональными обязанностями.

Технические решения

Для реализации концепции используются технологии:

- Шифрование данных для защиты информации в процессе передачи и хранения.
- Двухфакторная аутентификация для проверки идентичности пользователей.
- Виртуальные частные сети (VPN) для обеспечения безопасного соединения.
- Системы управления доступом для автоматизации политики доступа.

Постоянная оценка и аудит безопасности

Регулярное проведение аудита IT-инфраструктуры позволяет поддерживать актуальность политики безопасности и своевременно выявлять новые угрозы.

4. Преимущества реализации

Повышение уровня безопасности данных

Использование концепции нулевого доверия минимизирует риски утечек данных и несанкционированного доступа, что особенно важно для государственных систем, работающих с критически важной информацией.

Прозрачность и управляемость процессов

Zero Trust обеспечивает полный контроль над всеми аспектами взаимодействия с данными, что повышает управляемость IT-систем и способствует своевременному реагированию на угрозы.

Заключение. Концепция нулевого доверия представляет собой современный и эффективный подход к обеспечению безопасности государственных информационных систем. Она позволяет минимизировать риски несанкционированного доступа и утечек данных за счет строгой аутентификации, минимизации привилегий, сегментации сети и постоянного мониторинга активности. В условиях увеличения числа киберугроз и усложнения IT-инфраструктуры переход на архитектуру нулевого доверия становится не просто необходимым, но и стратегически важным шагом.

Внедрение принципов Zero Trust способствует повышению устойчивости функционирования государственных информационных систем, прозрачности и управляемости процессов, что особенно важно в условиях непрекращающихся атак на государственный сектор. Таким образом, реализация данной концепции позволит создать надежный барьер для киберугроз и обеспечит защиту критически важных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. "NIST Special Publication 800-207 Zero Trust Architecture" от 11.08.2020 № 800-207 2020

2. Архитектура сетевой безопасности Zero Trust: внедрение началось Источник: https://www.anti-malware.ru/analytics/Technology_Analysis/Zero-Trust-implementation-started // anti-malware URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Zero-Trust-implementation-started (дата обращения: 20.11.2024).

3. Концепция безопасности Zero Trust: преимущества и принцип работы // kaspersky URL: https://www.kaspersky.ru/resource-center/definitions/zero-trust (дата обращения:

16.11.2024).

4. Архитектура нулевого доверия (Zero Trust Architecture – ZTA) // Код безопасности URL: https://www.securitycode.ru/solutions/architecture-zta/ (дата обращения: 01.12.2024).

5. Иванов П.А., Капгер И.В., Шабуров А.С. МОДЕЛЬ РЕАЛИЗАЦИИ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ АКТИВАМ В КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. - 2023. - №45. - С. 147-163.

6. Безопасность данных с концепцией «нулевого доверия» // solar URL: https://rt-solar.ru/products/solar_dozor/blog/3824/ (дата обращения: 01.12.2024).

7. Zero Trust. Защита начинается с недоверия // it-world URL: https://www.it-world.ru/security/s4h4dwvfji80www4k8o8c4o80o8kw8w.html (дата обращения: 05.12.2024).

8. Что такое Zero Trust? Модель безопасности // habr URL: https://habr.com/ru/companies/varonis/articles/472934/ (дата обращения: 01.12.2024).

9. Microsoft Security // microsoft URL: https://learn.microsoft.com/ru-ru/security/zero-trust/ (дата обращения: 12.11.2024).

10. What is a Zero Trust Architecture] // Palo Alto. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zerotrust-architecture (дата обращения: 12.11.2024).

11. Киберугрозы в государственном секторе // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id1 (дата обращения: 08.12.2024).

12. Исследование Microsoft // microsoft URL: https://news.microsoft.com/ru-ru/microsoft-zero-trust-adoption-report-2021/ (дата обращения: 01.12.2024).

REFERENCES

1. “NIST Special Publication 800-207 Zero Trust Architecture” dated 08/11/2020 No. 800-207 2020

2. Zero Trust network security architecture: implementation has begun Source: https://www.anti-malware.ru/analytics/Technology_Analysis/Zero-Trust-implementation-started // anti-malware URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Zero-Trust-implementation-started (accessed on 20.11.2024).

3. Zero Trust security concept: advantages and working principle // kaspersky URL: https://www.kaspersky.ru/resource-center/definitions/zero-trust (date of access: 16.11.2024).

4. Zero Trust Architecture (ZTA) // Security Code URL: https://www.securitycode.ru/solutions/architecture-zta/ (date of access: 01.12.2024).

5. Ivanov P.A., Kapger I.V., Shaburov A.S. MODEL OF REALIZATION OF MANAGEMENT OF ACCESS TO INFORMATION ACTIVITIES IN THE ZERO TRUST CONCEPT // Bulletin of Perm National Research Polytechnic University. Electrical engineering, information technologies, control systems. - 2023. - №45. - C. 147-163.

6. Data security with the concept of “zero trust” // solar URL: https://rt-solar.ru/products/solar_dozor/blog/3824/ (date of reference: 01.12.2024).

7. Zero Trust. Protection begins with distrust // it-world URL: https://www.it-world.ru/security/s4h4dwvfji80www4k8o8c4o80o8kw8w.html (date of access: 05.12.2024).

8. What is Zero Trust? Security Model // habr URL: https://habr.com/ru/companies/varonis/articles/472934/ (accessed on 01.12.2024).

9. Microsoft Security // microsoft URL: https://learn.microsoft.com/ru-ru/security/zero-trust/ (accessed 12.11.2024).

10. What is a Zero Trust Architecture] // Palo Alto. - URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zerotrust-architecture (date of reference: 12.11.2024).

11. Cyber Threats in the Public Sector // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id1 (date of access: 08.12.2024).

12. microsoft research // microsoft URL: https://news.microsoft.com/ru-ru/microsoft-zero-trust-adoption-report-2021/ (date of access: 01.12.2024).

Информация об авторах

Михалева Ариана Дмитриевна – студент группы БиМ.1-24-1, кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: mihalevaarin@yandex.ru.

Сергей Петрович Серёдкин – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Mikhaleva Ariana Dmitrievna – student of the BiM-24-1 group, Department of Information Systems and Information Protection, Irkutsk State University of Railway Engineering, Irkutsk, e-mail: mihalevaarin@yandex.ru.

Sergei Petrovich Seryodkin – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Михалева А.Д., Серёдкин С.П. Концепция нулевого доверия как модель безопасности для государственной информационной системы // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №4. – С. 23-30. – Режим доступа: http://ismm-irgups.ru/toma/424-2024, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 09.12.2024)

For citations

Mikhaleva A.D., Seredkin S.P. The concept of zero trust as a security model for the state information system // "Information technologies and mathematical modeling in the management of complex systems": electron. Scientific journal – 2024. – No.4. – P. 23-30 – Access mode: http://ismm-irgups.ru/toma/424-2024, free. – Cover from the screen. – Yaz. rus., English (date of access: 09.12.2024)