Научная статья

DOI 10.15593/2224-9397/2023.1.07
УДК 004.056

П.А. Иванов[1], **И.В. Капгер**[2], **А.С. Шабуров**[2]

[1]Финансовый университет при Правительстве Российской Федерации, Москва, Россия
[2]Пермский национальный исследовательский политехнический университет, Пермь, Россия

МОДЕЛЬ РЕАЛИЗАЦИИ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ АКТИВАМ В КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ

Управление доступом к информационным активам – это одна из ключевых функций обеспечения информационной безопасности. Данная задача в том или ином виде должна решаться как в целом на уровне всей ИТ-инфраструктуры компании или организации, так и в каждой локальной информационной системе. В статье рассматривается процесс управления доступом к информационным активам в концепции нулевого доверия. «Нулевое доверие» удовлетворяет потребностям приложений, пользователей и устройств в быстром и безопасном доступе к данным в распределенных архитектурах. **Цель исследования:** разработка эффективной модели управления доступом, а также её описание в виде формализованной модели. **Результаты:** на основе существующих подходов разработана модель предоставления доступа к информационным активам, позволяющая реализовать процессы управления доступом в распределённой ИТ-инфраструктуре. Особенностью модели является алгоритм динамического определения требуемых политик безопасности, который учитывает доступ пользователей с различными привилегиями. В модели учитывается удалённый доступ на нескольких условных «уровнях» – доступ клиентов организации, сотрудников организации, а также партнеров и подрядных организаций. Поскольку современные информационные инфраструктуры организаций стали сложными и распределёнными, модель предполагает наличие значительного числа точек доступа, среди которых выделяются автоматизированные рабочие места внутри инфраструктуры, удаленные автоматизированные рабочие места, различные пользовательские и мобильные устройства доступа, а также специфические устройства типа торговых терминалов, эффективное управление доступом должно предоставлять возможность централизованного доступа всех пользователей к информационным активам. Она подразумевает реализацию единой входной точки доступа, построенной на основе моделей предоставления доступа из концепции нулевого доверия, для пользователей и для «роботов» –- технических учётных записей, которые используются для межсистемного взаимодействия. **Практическая значимость:** результаты исследования позволят разработать архитектуру удаленного доступа пользователей к распределённым информационным активам и организовать процессы контроля и управления доступом, в основе которых лежит динамическое определение уровня доверия к субъектам доступа, что в целом позволяет повысить защищённость организаций.

Ключевые слова: информационная безопасность, управление доступом, нулевое доверие.

P.A. Ivanov[1], I.V. Kapger[2], A.S. Shaburov[2]

[1]Financial university under the Government of the Russian Federation,
Moscow, Russian Federation
[2]Perm National Research Polytechnic University, Perm, Russian Federation

MODEL OF ACCESS MANAGEMENT TO INFORMATION ASSETS IN ZERO TRUST CONCEPT

Access control management to the information assets is one of the most important parts of cybersecurity. This problem in one form or another should be solved both as a whole at the level of entire IT-infrastructure of a company or organization, and in each local information system. This article describes the process of access management to information assets based on the concept of zero trust. "Zero trust" concept meets the requirements of applications, users and devices in fast and secure access to data in distributed architectures. **Purpose:** to develop an effective model of access management and to describe it in a form of formalized model. **Results:** development on existing approaches base of an access control management model, which allows to implement access control processes in a distributed IT infrastructure. A distinguishing feature of the proposed model is offering an algorithm of dynamic security policies determination which takes into account an access of subjects with different level of privileges. The model takes into account few conditional levels of remote access – access of company's clients, employees and contractors. Given a complex and distributed character of modern information infrastructures of organizations, the model implies the existence of a significant number of access points with automated workstations within the infrastructure, remote workstations, various personal and mobile devices, as well as specific devices such as trading terminals, to name just a few. An effective access control should provide the possibility of centralized access to information assets for all users. It implies the use of a single entry point built on the basis of access models from the concept of "zero trust". **Practical relevance:** the results of the research can be used in development of architecture for remote user access to distributed information assets and organizing access control and management processes based on dynamic determination of the trust level of access subjects, which, in general, improves the security of organizations.

Keywords: cybersecurity, access management, zero trust.

Введение

Современные темпы разработки и развития информационных технологий в значительной степени поддерживаются требованиями различных институтов использовании актуальных и эффективных ИТ-решений, внедряемых в функциональные процессы, которые нуждаются в улучшении, оптимизации и модернизации в соответствии с требованиями потребителей информационных услуг. Государственные учреждения и частные организаций стали нуждаться в обеспечении безопасности информационной инфраструктуры из-за внедрения новых технологий, которые требовали совмещения с существующими и устаревшими технологиями, а также распространения облачных вычислений [1–4]. В ответ на потребность пересмотра подхода к построению их архитектуры появилась концепция нулевого доверия, изложен-

ная в стандарте Национального института стандартов и технологий (NIST) [5, 6]. Она была создана с осознанием того, что традиционные модели безопасности построены на устаревшем постулате о доверии всему внутри сети организации [7, 8].

«Нулевое доверие» удовлетворяет потребностям приложений, пользователей и устройств в быстром и безопасном доступе к данным в распределенных архитектурах. За счёт использования концепции может быть построена гибкая и непрерывная защита пользователей и информационных активов в случаях, когда нельзя быть уверенным в безопасности сети. Такая концепция призывает изначально не доверять и реализовывать проверку безопасности каждого пользователя, устройства или сеанса доступа в каждом конкретном запросе к информационному активу [9, 10]. Концепция нулевого доверия представляет собой совокупность идей, которые призваны увеличить уверенность при принятии решения о предоставлении доступа для каждого запроса в рамках недоверенной сети. Основной её целью являются предотвращение несанкционированного доступа и максимально возможная детализация контроля доступа [11, 12], при этом концепция предлагает подход, а не конкретные алгоритмы и модели реализации контроля доступа.

Целью статьи является разработка формальной модели управления доступом к информационным активам, рассматриваемой в рамках концепции нулевого доверия, которая стала очень актуальной с переходом на периметр информационных систем, основанный на распределенных информационных активах, а не на защищённом контуре. В рамках исследования ставятся задачи изучения существующих моделей управления доступом и формирования на их основе более комплексной модели, которая будет подразумевать динамическую проверку полномочий субъектов доступа с разными привилегиями в запрашиваемой системе.

В качестве объекта исследования выбрана распределённая информационная инфраструктура, для которой требуется организация процесса управления доступом к информационным активам. Примером такой инфраструктуры может быть любая современная крупная компания в сфере информационных технологий или крупная финансовая организация. Поскольку «размытие» периметра защиты требует проработки иного решения для контроля доступа, так как локальный доступ дополняется удалённым доступом от различных узлов, находящихся за рамками контролируемой сети, возникает необходимость выбора наиболее эффективной модели контроля и управления доступом

в условиях, когда субъект доступа может как доверенным, так и недоверенным. Нулевое доверие устраняет различия между подобными субъектами доступа [13, 14].

Понятие концепции нулевого доверия

Фактически концепция нулевого доверия – это набор концепций, который призван минимизировать уровень неопределённости при решении о предоставлении доступа к информационному ресурсу в потенциально незащищённых сетях, который удовлетворяет требованиям минимальных привилегий.

Следует подчеркнуть, что планирование приведения инфраструктуры в соответствие с принципами нулевого доверия невозможно произвести частично или в рамках доработки информационных систем. Требуется перестроение информационной инфраструктуры в целом, а также интеграция во все аспекты деятельности организации, чтобы принципы нулевого доверия показали свою эффективность [15, 16]. При этом наибольшая эффективность достигается при вложении достаточных средств и увеличении инвестиций в процессы поддержания инфраструктуры нулевого доверия [17].

Основа концепции заложена в NIST Special Publication 800-207 [5], которая может быть использована в качестве руководства для проработки и внедрения ZTA (ZeroTrustAccess, доступа с нулевым доверием) в организациях. В данной публикации также приведена абстрактная логическая модель архитектуры нулевого доверия (рис. 1), которая была использована в качестве базиса для разрабатываемой модели реализации управления доступом.

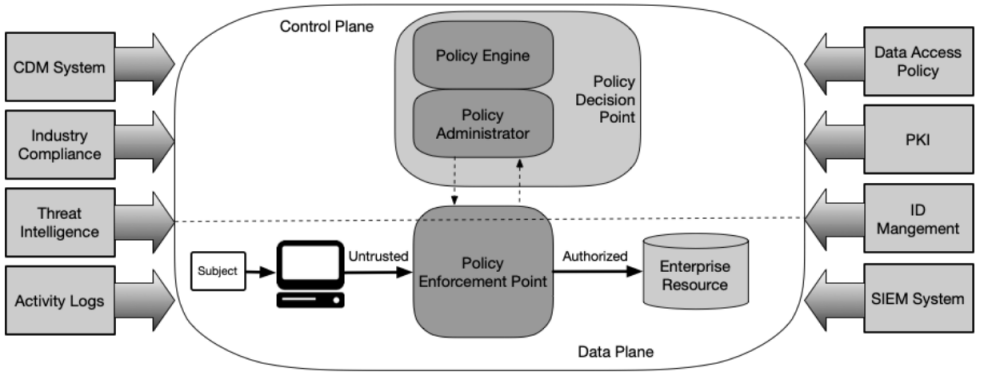

Рис. 1. Основные логические компоненты модели нулевого доверия (NIST SpecialPublication 800-207)

Основными элементами данной модели являются [5]:

– 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.

Принципы предоставления доступа к информационным активам

В основу предоставления доступа закладываются принципы, изложенные в той же концепции [5], которые могут быть коротко сформулированы следующим образом:

1) аутентификация и авторизация всех субъектов доступа является динамической и обязательной;

2) все источники данных и сервисы – это предварительно учтённые ресурсы;

3) состояние безопасности и целостность всех информационных ресурсов постоянно контролируются;

4) все взаимодействия защищены независимо от принадлежности к сети;

5) доступ к конкретным информационным ресурсам предоставляется в рамках соответствующей такому доступу сессии;

6) решение о предоставлении доступа принимается на основании динамических политик, учитывающих данные, полученные по PIPs;

7) обеспечивается сбор максимально возможных объемов данных о состоянии защищённости информационных активов, сетевой инфраструктуры и субъектов доступа.

Перечисленные принципы являются базовыми и должны быть соблюдены при реализации концепции нулевого доверия в организации. Однако в рамках исследования рассматривается не абстрактная ситуация предоставления доступа некоему субъекту, а конкретным группам пользователей со своей спецификой, т.е. субъектам с разными полномочиями в информационных активах – пользовательскими и административными, а также специфическим субъектам – внешним сервисам.

Для субъектов, требующих более широких полномочий или административного доступа, подразумевается применение специализированных методов и инструментов обеспечения безопасности доступа таких субъектов. Поэтому помимо основных принципов концепции нулевого доверия также были определены два следующих принципа:

1) для предоставления более широких привилегий в рамках сеанса доступа требуется выполнение более строгих политик;

2) формирование политик PE должно осуществляться с учетом максимально возможной степени защищенности и целостности субъектов доступа.

Первый дополнительный принцип заложен, исходя из особенностей предоставления доступа субъектам, выполняющим административные функции, поскольку данные функции требуют предоставления избыточных полномочий, выходящих за рамки минимально необходимых. Доступ таких субъектов, как правило, осуществляется при проведении дополнительных мероприятий по проверке устройств, с которых осуществляется доступ, контроля такого доступа и его мониторинга.

Второй дополнительный принцип закладывается, исходя из вероятных ограничений, которые могут присутствовать при запросе доступа со стороны технических сервисов, так как различные технологии, используемые для реализации доступа, могут объективно не иметь возможности выполнить требования основных политик PE. Требуется

формировать их с учётом каждого конкретного технического сервиса и обеспечивать доступ к минимально необходимым информационным ресурсам.

Типы субъектов доступа, рассматриваемых в рамках модели

Национальный институт стандартов и технологий предлагает несколько основных моделей внедрения архитектуры нулевого доверия, которые в общем виде описывают, каким образом может быть реализована информационная инфраструктура организации. В рамках исследования рассматривается сценарий управления доступом, который включает в себя несколько типов субъектов доступа, к которым не может быть применен ни один из существующих вариантов реализации архитектуры нулевого доверия из стандарта:

1) клиенты организации;
2) сотрудники организации;
3) подрядчики и внешние разработчики;
4) партнеры и контрагенты организации;
5) государственные организации и регуляторы.

Первые три группы объединяют в себе пользовательский доступ к информационным системам со стороны субъектов, которые используют существующие каналы доступа и имеют различный перечень доступных каналов (финансовые сервисы, системы дистанционного банковского обслуживания, системы контакт-центра и т.п., доступ к автоматизированным рабочим местам, доступ к средам разработки и тестовым контурам организации), а также различный уровень привилегий в рамках этих каналов.

Оставшиеся группы – это специфические субъекты доступа, требующие предоставления каналов доступа к информационным сервисам, а также к закрытым сервисам предоставления конфиденциальной информации, причем часто к таким каналам предъявляются и специфические требования, продиктованные как соблюдением законодательства в сфере защиты информации, так и особенностями информационных систем субъектов доступа.

Основной проблемой, которую необходимо решить, является гетерогенность каналов доступа для определённых типов субъектов. Доступ каждой из групп субъектов доступа не может быть реализован через единый механизм предоставления доступа, одного провайдера

аутентификации и единый перечень политик, что ставит вопрос проработки модели предоставления доступа, в которую будут заложены перечисленные особенности.

Модель реализации доступа к информационным активам

В основу разрабатываемой модели предоставления доступа заложена модель, представленная на рис. 2.

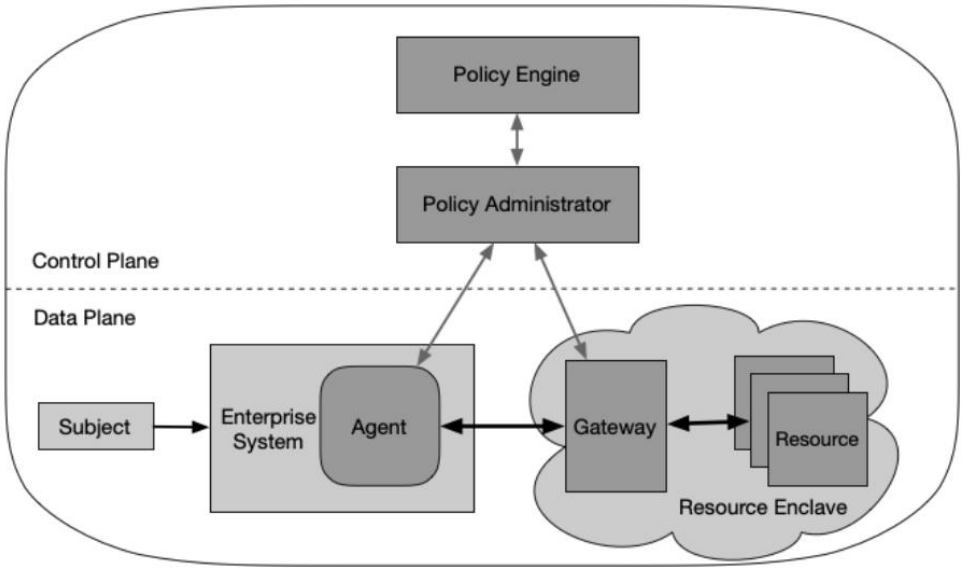

Рис. 2. Модель шлюза анклава (NIST SP 800-207 Zero Trust Architecture)

Она предполагает использование следующих логических компонентов:

– агент, расположенный на ресурсе, с которого осуществляется запрос доступа;

– шлюз, который является входной точкой доступа к информационным ресурсам.

Информационные ресурсы, расположенные за шлюзом, не являются одиночными (как, например, веб-сервис), а представляют собой «анклав» – совокупность информационных активов, расположенных на одних и тех же вычислительных ресурсах.

В этой модели присутствует агент на субъекте доступа, который используется для подключения к шлюзу «анклава» и может представлять собой агента специфической системы защиты информации, которая позволит, например, обеспечить контроль привилегированного

доступа. С использованием агента можно обеспечить реализацию политик точечного доступа к определённому ресурсу, а использование шлюза обеспечивает контроль доступа сразу к перечню информационных ресурсов, что даёт возможность реализации политик для пользователей с разными привилегиями.

Недостатком данной модели является то, что шлюз обеспечивает безопасность ресурсов анклава в целом и может не обеспечивать безопасность отдельных из них, тем самым дает субъектам доступа потенциальную возможность обнаружения ресурсов внутри анклава, к которым у них отсутствует правомерный доступ. Разработанная в рамках исследования модель (рис. 3) представляет собой усложнённую версию «модели шлюза анклава», которая характеризуется более сложными механизмами предоставления доступа через шлюз для всех вышеупомянутых групп субъектов доступа.

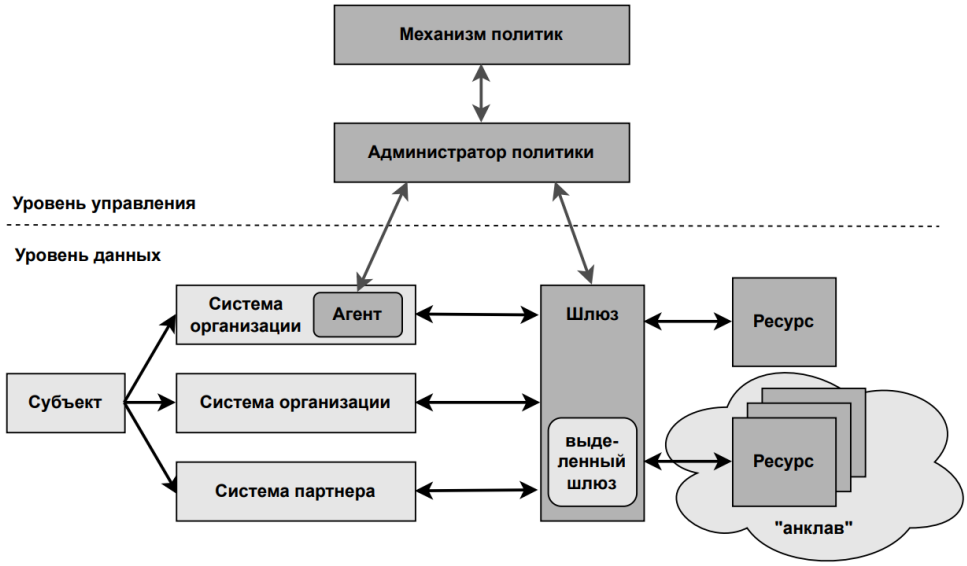

Рис. 3. Разработанная модель реализации управления доступом

Субъект доступа может осуществлять запросы доступа с корпоративной системы с установленным агентом или без него, а также с условно внешних систем партнера. Каждый запрос доступа обрабатывается на шлюзе, который является точкой применения политик, при этом запросы от систем партнера обрабатываются на выделенной части шлюза, для которого применяются иные политики со стороны механизма политик.

На рис. 4 представлена диаграмма маршрутизации запроса доступа через шлюз. Запрос доступа поступает через балансировщик, поскольку шлюз является составным объектом в модели. Для каждого запроса на основании данных о состоянии защищённости, поступающих от PIPs, определяются источник запроса и дальнейший путь обработки – каким компонентом шлюза он будет получен для выполнения. Далее на основании политик доступа производятся идентификация и аутентификация, в случае успеха которых формируется запрос авторизации.

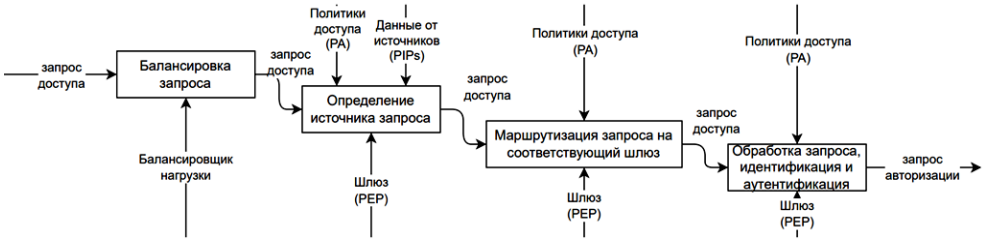

Рис. 4. Диаграмма маршрутизации запроса доступа через PEP

Идентификация – это первый этап в рамках предоставления доступа и одновременно основа концепции нулевого доверия [18]. Аутентификация может быть реализована разными способами, при этом добавление второго фактора аутентификации может дополнительно снизить риски атак на систему управления доступом [19]. После успешного прохождения аутентификации условно формируется запрос авторизации, который подлежит дальнейшей обработке, диаграмма которой представлена на рис. 5.

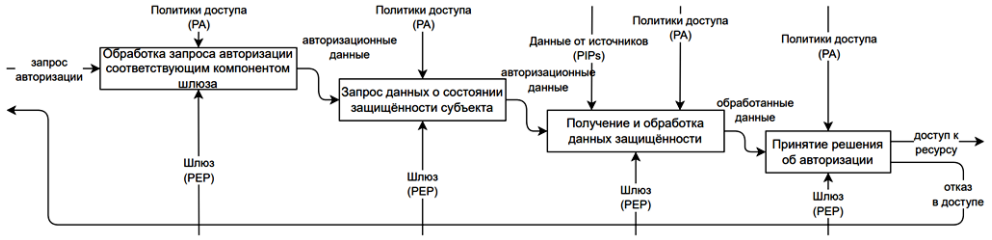

Рис. 5. Обработка запроса доступа через PEP

Особенностью предлагаемой схемы обработки является повторное обращение к информационным потокам PIPs, которые предоставляют имеющиеся данные о текущем состоянии защищённости субъекта доступа в момент авторизации. Таким образом, подразумевается

принятие решения о предоставлении доступа с двумя этапами проверки субъекта – в момент обработки запроса на идентификацию и аутентификацию, а также после успешного прохождения аутентификации, что позволит повысить уверенность в том, что данный запрос доступа легитимен и не принесёт рисков информационной безопасности.

Двойная проверка субъекта в рамках обработки запроса доступа обеспечивает гибкость при принятии решения на стороне PEP, а также позволяет использовать различные политики, которые, в зависимости от типа субъекта доступа, могут быть как более строгими, так и менее строгими. Слабые или недостаточно проработанные политики управления, согласно исследованию Verizon [20], приводят к большинству инцидентов, связанных с компрометацией учётных записей, а согласно отчёту XMCyber [21], 73 % наиболее распространенных методов атак связаны с некорректными механизмами управления доступом или скомпрометированными аккаунтами. С использованием комплексных динамических политик возможна реализация управления доступом, снижающая риски нарушения безопасности до минимума.

Нулевое доверие в целом позволяет уменьшать возможную поверхность атаки и снижать уровень ущерба, а также последствия кибератак за счёт сокращения времени и затрат на управление угрозами безопасности. Высокая степень прозрачности при предоставлении доступа упрощает процессы администрирования и снижает риски несанкционированного доступа, поскольку его могут получить только те субъекты, которые на основании ряда проверок подтвердили свой уровень защищённости [22, 23]. Кроме того, унификация политик доступа для приложений и серверов, являющихся критически важной частью ИТ-инфраструктуры, является ключом к объединению IAM в единое безопасное и управляемое место для ИТ-подразделений в локальной среде и в облаке [24, 25].

Предложенная модель предоставления доступа не лишена недостатков модели-прототипа, но в отличие от неё предоставляет возможность доступа через шлюз к отдельным информационным ресурсам, а также ресурсам в анклаве, что подразумевает реализацию на PE более сложных и универсальных политик, которые будут заложены на администраторе политики. За счёт этого возможно построение защищённых реальных архитектур, в которых будут заложены различные пути доступа к целевым информационным ресурсам. Это привносит

сложности для администрирования и разработки политик, однако данный факт нельзя считать недостатком модели, поскольку концепция нулевого доверия подразумевает постоянный пересмотр политик и изменение информационной инфраструктуры. Это сам по себе сложный процесс, требующий от архитектуры нулевого доверия, способности подстраиваться под вносимые изменения. В рамках дальнейших исследований возможны детальная проработка процесса предоставления доступа и разработка политик доступа на основании динамических данных о состоянии защищённости субъектов доступа.

Библиографическийсписок

1. Garbis J. Chapman J.W. Zero Trust Security: An Enterprise Guide. – Springer: Berlin/Heidelberg, Germany, 2021.

2. Карр Николас. Великий переход: что готовит революция облачных технологий. – М.: Машиностроение, 2019. – 722 с.

3. Жданович О.А. Система обеспечения бизнес-процессов расходными материалами на основе облачных технологий. – М.: Синергия, 2017. – 377 с.

4. Щербатский В.Б., Кормышев В.М. Облачные технологии в обучении и оценке компетентности специалистов. – М.: LAPLambertAcademicPublishing, 2018. – 152 с.

5. NIST Special Publication 800-207 Zero Trust Architecture. – August 2020. – 59 p.

6. Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow NIST Enterprise Architecture Model // Book language. English; Published on. 2010-11-20; Publishing house.

7. What is a Zero Trust Architecture [Электронныйресурс] // Palo Alto. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (дата обращения: 05.02.2023).

8. Модель архитектуры предприятия NIST – NIST Enterprise Architecture Model [Электронный ресурс]. – URL: https://ru.wikibrief.org/wiki/NIST_Enterprise_Architecture_Model (дата обращения: 05.02.2023).

9. Whatiszerotrust? [Электронный ресурс]. – URL: https://www.ibm.com/topics/zero-trust (дата доступа: 04.02.2023).

10. Кузнецов С.А., Куликов И.А., Фоминых А.А. Модель нулевого доверия применительно к корпоративным информационным

системам // Актуальные научные исследования в современном мире. – 2021. – № 6-1 (74). – С. 59–62.

11. Что такое нулевое доверие? [Электронный ресурс]. – URL: https://www.trendmicro.com/ru_ru/what-is/what-is-zero-trust.html (дата обращения: 04.02.2023).

12. Реализация архитектуры безопасности с нулевым доверием: вторая редакция [Электронный ресурс]. – URL: https://habr.com/ru/company/vk/blog/498332/ (дата обращения: 06.02.2023).

13. NIST CSWP 20 Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. – May 6, 2022. – 14 p.

14. Обзор публикации NIST SP 800-207 "Zero Trust Architecture" [Электронный ресурс] / Руслан Рахметов. – Security Vision. – URL: https://www.securityvision.ru/blog/obzor-publikatsii-nist-sp-800-207-zero-trust-architecture/ (дата обращения: 06.02.2023).

15. Why Zero Trust cybersecurity relies on people as much as tech [Электронный ресурс]. – URL: https://translated.turbopages.org/proxy_u/en-ru.ru.8cd49db8-64045964-a7ffcf95-74722d776562/https/www.techradar.com/opinion/why-zero-trust-cybersecurity-relies-on-people-as-much-as-tech (дата обращения: 07.02.2023).

16. Wagenseil P. How identity and access management fits into zero trust [Электронный ресурс]. – URL: https://www.scmagazine.com/resource/identity-and-access/how-identity-and-access-management-fits-into-zero-trust (дата обращения: 08.02.2023).

17. Политика «нулевого доверия»: осторожность окупается! [Электронный ресурс]. – URL: https://softline.kz/about/news/politika-nulevogo-doveriya-ostorozhnost-okupaetsya (дата обращения: 08.02.2023).

18. The path to zero trust starts with identity [Электронный ресурс]. IDSA. – URL: https://www.idsalliance.org/white-paper/the-path-to-zero-trust-starts-with-identity/ (дата обращения: 07.02.2023).

19. Getting Started with Zero Trust Access Management Trust Begins with Secure Identity [Электронный ресурс]. – Okta. – URL: https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/ (дата обращения: 07.02.2023).

20. 2022 Data Breach Investigations Report [Электронный ресурс]. Verizon. – URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 08.02.2023).

21. 2022 Exposure management impact report [Электронный ресурс]. – XM Cyber. – URL: https://info.xmcyber.com/2022-attack-path-management-impact-report (дата обращения: 07.02.2023).

22. Полянский Д.А. Оценка защищенности: учеб. пособие. – Владимир: Изд-во Владим. гос. ун-та, 2005. – 80 с.

23. Яцкевич А.И., Кошелев С.О. Аналитические методы оценки защищенности информации, обрабатываемой в информационной системе // Молодой ученый. – 2016. – № 28 (132). – С. 45–49. – URL: https://moluch.ru/archive/132/36917/ (дата обращения: 05.03.2023).

24. Zero trust architecture explained [Электронный ресурс]. – Zscaler. – URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust (дата обращения: 07.02.2023).

25. Сапрыкина А. Как управлять доступом к корпоративным ресурсам с помощью платформы Makves [Электронный ресурс]. – Anti-malware. – URL: https://www.anti-malware.ru/practice/methods/Identity-and-Access-Governance-with-Makves-DCAP (дата обращения: 07.02.2023).

References

1. Garbis J. Chapman J.W. Zero Trust Security: An Enterprise Guide. Springer: Berlin/Heidelberg, Germany, 2021.

2. Karr Nikolas. Velikii perekhod: chto gotovit revoliutsiia oblachnykh tekhnologii [The Great Transition: What the Cloud Technology Revolution is preparing]. Moscow: Mashinostroenie, 2019, 722 p.

3. Zhdanovich O.A. Sistema obespecheniia biznes-protsessov raskhodnymi materialami na osnove oblachnykh tekhnologii [A system for providing business processes with consumables based on cloud technologies]. Moscow: Sinergiia, 2017, 377 p.

4. Shcherbatskii V.B., Kormyshev V.M. Oblachnye tekhnologii v obuchenii i otsenke kompetentnosti spetsialistov [Cloud technologies in the training and assessment of the competence of specialists]. Moscow: Lambert Academic Publishing, 2018, 152 p.

5. NIST Special Publication 800-207 Zero Trust Architecture. August 2020, 59 p.

6. Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow NIST Enterprise Architecture Model. Book language. English; Published on. 2010-11-20; Publishing house.

7. What is a Zero Trust Architecture. *Palo Alto*. available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (accessed 05 February 2023).

8. Model' arkhitektury predpriiatiia NIST- NIST Enterprise Architecture Model [NIST Enterprise Architecture Model- NIST Enterprise Architecture Model], available at: https://ru.wikibrief.org/wiki/NIST_Enterprise_Architecture_Model (accessed 05 February 2023).

9. Whatiszerotrust? available at: https://www.ibm.com/topics/zero-trust (accessed 04 February 2023).

10. Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Model' nulevogo doveriia primenitel'no k korporativnym informatsionnym sistemam [Zero trust model applied to corporate information systems]. *Aktual'nye nauchnye issledovaniia v sovremennom mire*, 2021, no. 6-1 (74), pp. 59-62.

11. Chto takoe nulevoe doverie? [What is zero trust?], available at: https://www.trendmicro.com/ru_ru/what-is/what-is-zero-trust.html (accessed 04 February 2023).

12. Realizatsiia arkhitektury bezopasnosti s nulevym doveriem: vtoraia redaktsiia [Implementation of a zero-trust security architecture: second edition], available at: https://habr.com/ru/company/vk/blog/498332/ (accessed 06 February 2023).

13. NIST CSWP 20 Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. May 6, 2022, 14 p.

14. Рахметов Р. Обзор публикации NIST SP 800-207 "Zero Trust Architecture" [Обзор публикации NIST SP 800-207 "Zero Trust Architecture"]. Security Vision, available at: https://www.securityvision.ru/blog/obzor-publikatsii-nist-sp-800-207-zero-trust-architecture/ (accessed 06 February 2023).

15. Why Zero Trust cybersecurity relies on people as much as tech, available at: https://translated.turbopages.org/proxy_u/en-ru.ru.8cd49db8-64045964-a7ffcf95-74722d776562/https/www.techradar.com/opinion/why-zero-trust-cybersecurity-relies-on-people-as-much-as-tech (accessed 07 February 2023).

16. Wagenseil P. How identity and access management fits into zero trust, available at: https://www.scmagazine.com/resource/identity-and-access/how-identity-and-access-management-fits-into-zero-trust (accessed 08 February 2023).

17. Politika “nulevogo doveriia”: ostorozhnost' okupaetsia! [The policy of “zero trust": caution pays off!], available at: https://softline.kz/about/

news/politika-nulevogo-doveriya-ostorozhnost-okupaetsya (accessed 08 February 2023).

18. The path to zero trust starts with identity. IDSA, available at: https://www.idsalliance.org/white-paper/the-path-to-zero-trust-starts-with-identity/ (accessed 07 February 2023).

19. Getting Started with Zero Trust Access Management Trust Begins with Secure Identity. Okta, available at: https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/ (accessed 07 February 2023).

20. 2022 Data Breach Investigations Report. Verizon, available at: https://www.verizon.com/business/resources/reports/dbir/ (accessed 08 February 2023).

21. 2022 Exposure Management Impact Report. XM Cyber, available at: https://info.xmcyber.com/2022-attack-path-management-impact-report (accessed 07 February 2023).

22. Polianskii D.A. Otsenka zashchishchennosti [Security assessment]. Vladimir: Vladimirskii gosudarstvennyi universitet, 2005, 80 p.

23. Iatskevich A.I., Koshelev S.O. Analiticheskie metody otsenki zashchishchennosti informatsii, obrabatyvaemoi v informatsionnoi sisteme [Analytical methods for assessing the security of information processed in an information system]. *Molodoi uchenyi*, 2016, no. 28 (132), pp. 45-49, available at: https://moluch.ru/archive/132/36917/ (accessed 05 March 2023).

24. Zero Trust Architecture Explained. Zscaler, available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust (accessed 07 February 2023).

25. Saprykina A. Kak upravliat' dostupom k korporativnym resursam s pomoshch'iu platformy Makves [How to manage access to corporate resources using the Makes platform]. Anti-malware, available at: https://www.anti-malware.ru/practice/methods/Identity-and-Access-Governance-with-Makves-DCAP (accessed 07 February 2023).

Сведения об авторах

Иванов Павел Алексеевич (Москва, Россия) – аспирант Департамента информационной безопасности, Финансовый университет при Правительстве Российской Федерации (Москва, e-mail: 218666@edu.fa.ru).

Капгер Игорь Владимирович (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: kapger@mail.ru).

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

About the authors

Pavel A. Ivanov (Moscow, Russian Federation) – Graduate Student of the Department of Information Security. Financial University under the Government of the Russian Federation, Moscow, e-mail: 218666@edu.fa.ru

Igor V. Kapger (Perm, Russian Federation) – Ph. D of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: kapger@mail.ru).

Andrey S. Shaburov (Perm, Russian Federation) – Ph. D of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Поступила: 24.10.2022. Одобрена: 03.11.2022. Принята к публикации: 01.04.2023.

Финансирование. Исследование не имело спонсорской поддержки.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов. Все авторы сделали эквивалентный вклад в подготовку публикации.

Просьба ссылаться на эту статью в русскоязычных источниках следующим образом:

Иванов, П.А. Модель реализации управления доступом к информационным активам в концепции нулевого доверия / П.А. Иванов, И.В. Капгер, А.С. Шабуров // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2023. – № 45. – С. 147–163. DOI: 10.15593/2224-9397/2023.1.07

Please cite this article in English as:

Ivanov P.A., Kapger I.V., Shaburov A.S. Model of access management to information assets in zero trust concept. *Perm National Research Polytechnic University Bulletin. Electrotechnics, information technologies, control systems*, 2023, no. 45, pp. 147-163. DOI: 10.15593/2224-9397/2023.1.07