ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES

УДК 004.75
DOI: 10.37661/1816-0301-2024-21-4-85-98

Обзорная статья
Review Article

К вопросу проектирования компьютерных систем на основе архитектуры нулевого доверия

А. И. Бражук✉, Е. В. Олизарович

Гродненский государственный университет имени Янки Купалы,
ул. Ожешко, 22, Гродно, 230023, Беларусь
✉*E-mail: brazhuk@grsu.by*

Аннотация
Работа посвящена теоретическим и практическим аспектам проектирования компьютерных систем, базирующихся на концепции нулевого доверия. На основе системного подхода к анализу существующих систем нулевого доверия и теоретических моделей, используемых при их проектировании, в работе сформулированы ключевые проблемы реализации систем нулевого доверия. Также в рамках дисциплины шаблонов проектирования и безопасности рассмотрены принципиальное представление концепции нулевого доверия и абстрактная модель (шаблон) контроля доступа архитектуры нулевого доверия.
Принципиальное представление может быть использовано для формализации абстрактных шаблонов проектирования и безопасности, а шаблон контроля доступа – для создания производных шаблонов и архитектур компьютерных систем на основе концепции нулевого доверия. Важная особенность шаблона контроля доступа заключается в возможности полнее формулировать функциональные требования и представлять архитектуры проектируемых систем за счет описания уровней контроля доступа (сетевой путь, сессия, транзакция).

Ключевые слова: компьютерные системы, шаблоны проектирования, шаблоны безопасности, нулевое доверие, архитектура нулевого доверия, информационная безопасность

Для цитирования. Бражук, А. И. К вопросу проектирования компьютерных систем на основе архитектуры нулевого доверия / А. И. Бражук, Е. В. Олизарович // Информатика. – 2024. − Т. 21, № 4. – С. 85–98. – DOI: 10.37661/1816-0301-2024-21-4-85-98.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 22.07.2024
Подписана в печать | Accepted 22.08.2024
Опубликована | Published 30.12.2024

Towards the computer systems design based on Zero Trust Architecture

Andrei I. Brazhuk✉, Evgeny V. Olizarovich

Yanka Kupala State University of Grodno,
st. Ozheshko, 22, Grodno, 230023, Belarus
✉*E-mail: brazhuk@grsu.by*

Abstract
The work is devoted to theoretical and practical aspects of computer systems design based on the zero trust concept. Based on the system thinking of analyzing existing zero trust systems and theoretical models used in their design, the work describes key problems of implementing zero trust systems. Also, based on design and security patterns, the principles representation of the zero trust concept and the abstract access control model (pattern) of the Zero Trust Architecture are considered.
The principles representation can be used to mine abstract design and security patterns, and the access control pattern – to create derivative patterns and architectures of computer systems based on zero trust. An advance of the access control pattern is the capacity to more fully formulate functional requirements and represent the architectures of the designed systems due to the description of access control levels (network path, session, transaction).

Keywords: computer systems, design patterns, security patterns, zero trust, Zero Trust Architecture, information security

For citation. Brazhuk A. I., Olizarovich E. V. *Towards the computer systems design based on Zero Trust Architecture.* Informatika [*Informatics*], 2024, vol. 21, no. 4, pp. 85–98 (In Russ.). DOI: 10.37661/1816-0301-2024-21-4-85-98.

Conflict of interest. The authors declare of no conflict of interest.

Введение. Нулевое доверие (НД) является популярной концепцией информационной безопасности, определяющей, как должны строиться корпоративные системы защиты [1]. В ее основе лежит идея об отсутствии доверия со стороны информационных сервисов организации не только к интернет-пользователям, но и сотрудникам, находящимся в корпоративной сети.

Актуальность концепции НД обусловлена сменой моделей использования компьютерных ресурсов и способов доступа к ним. Облачные вычисления позволяют гибко размещать корпоративные сервисы как внутри периметра организации, так и в сети Интернет, а также использовать сторонние информационные ресурсы по подписке. Широкое распространение мобильных и переносимых компьютеров сделало возможным использование сотрудниками личных смартфонов и ноутбуков для доступа к корпоративным приложениям. Дополнительные сложности с точки зрения информационной безопасности создают системы интернета вещей и киберфизические системы, интегрированные в инфраструктуры информационных технологий организаций. В этих условиях традиционная концепция периметра безопасности утрачивает свое значение и на первый план выходят средства и методы защиты, ориентированные на конечные компьютерные системы.

Основная проблема концепции НД связана с широкой ее трактовкой и, как следствие, – большим количеством различных интерпретаций в научной литературе, интернет-источниках и брошюрах производителей средств защиты. Настоящая работа направлена на устранение имеющихся неоднозначностей и возможных противоречий путем, во-первых, анализа существующих проблем реализации архитектур НД; во-вторых, описания концепции НД посредством принципов информационной безопасности и, в-третьих, разработки шаблона проектирования, определяющего в общем виде функцию контроля доступа к ресурсам как основополагающую в корпоративных системах защиты на основе концепции НД. Шаблоны проектирования являются общепризнанным инструментом, позволяющим формализовать лучшие практики разработки архитектур компьютерных систем и сетей, что обеспечивает многократное использование опыта экспертов и специалистов в области информационной безопасности.

Нулевое доверие и архитектура нулевого доверия. В настоящее время НД связывают с защитой информационных ресурсов на основе предположения о том, что «доверие» (trust) к субъектам и объектам сетевых взаимодействий должно быть минимальным (отсутствовать), при этом контроль доступа является непрерывным и адаптивным процессом [1].

Распространение концепции НД (Zero Trust, ZT) началось в области компьютерных сетей (сетевой подход к НД) в рамках смены акцента с безопасного сетевого периметра к защите конечных устройств [2] ввиду необходимости внедрения методов и средств информационной безопасности, ориентированных на данные, передаваемые по сети. В качестве основной цели был заявлен переход к гибким сетевых архитектурам, обеспечивающим защиту данных, пользователей и приложений. Известен ряд дополнений оригинальной концепции НД [2], в частности сетевой доступ с НД (Zero Trust Network Access, ZTNA) [3], добавляющий проверку учетных данных пользователей при доступе к приложениям, и расширение НД (Zero Trust eXtended, ZTX) [4], распространяющее НД на данные, сети, людей, рабочие станции и устройства.

Сетевой подход к НД и его производные, как правило, основаны на микросегментации [5, 6], представляющей собой гранулирование сегментов сети с определенным уровнем доступа, вплоть до отдельных рабочих станций или серверов; централизации управления и защиты сети, связанной с внедрением проактивных средств защиты, таких как системы предотвращения вторжений [7], использованием данных о киберугрозах [8] и технологий сетевой автоматизации; средствах контроля доступа уровня сети, например аутентификации IEEE 802.1X и многофакторной аутентификации [9]. В исторической перспективе производители средств защиты в той или иной степени следуют сетевому подходу к НД в устройствах и программном обеспечении шлюзов безопасности (Security Gateway, SG), средствах унифицированного управления угрозами (Unified Threat Management, UTM), межсетевых экранах следующего поколения (Next Generation FireWall, NGFW) [10], а также облачных сервисах защиты (Security-as-a-Service, SECaaS) [11].

Примерами успешной реализации сетевого подхода к НД могут быть продукты, позиционируемые как решения для виртуализации сети, обеспечивающие абстрагирование сетевых функций от физической инфраструктуры для задач аппаратной виртуализации, контейнеризации и облачных вычислений [12]. Ключевой технологией в них является микросегментация, дополненная динамическими автоматическими политиками доступа.

Концепция программно-определяемых сетей (Software Defined Network, SDN) и технологии виртуализации сетевых функций (Network Functions Virtualization, NFV) открыли новые перспективы для реализации систем НД [13, 14]. Для архитектуры программно-определяемых сетей характерно разделение на уровень данных (Data Plane), непосредственно обеспечивающий передачу данных, и уровень управления (Control Plane), средства которого реализованы программно и способны тесно взаимодействовать с приложениями и сервисами, использующими сеть. Потенциальные возможности по управлению сетью, предоставляемые посредством SDN-контроллера приложениям, позволяют гибко удовлетворять их потребности и более точно контролировать доступ пользователей к приложениям.

Архитектура НД (Zero Trust Architecture, ZTA) предполагает обеспечение полного и продолжительного контроля сетевого доступа субъектов к объектам (ресурсам) [1]. На практике термин «архитектура нулевого доверия» (АНД) связывают с прикладным подходом к НД, так как в этом случае контроль доступа осуществляется на уровне приложений [15].

Пилотный проект [16], в котором был реализован прикладной подход к НД, сфокусирован на контроле доступа и управлении устройствами. Основная его идея заключалась в исключении привилегированного периметра и переносе корпоративных приложений в Интернет с обеспечением доступа к ним авторизованным корпоративным субъектам. Система контроля доступа управляла информационными потоками между пользователями и корпоративными ресурсами на основе динамической оценки доверия, принимающей в расчет данные как базы пользователей, так и базы устройств. Реализация использовала общеизвестные компоненты, такие как прикладной прокси, технология единого входа SSO, расширенный протокол удаленной аутентификации пользователей RADIUS и т. д.

Программно-определяемый периметр (Software Defined Perimeter, SDP) [17] следует рассматривать как пример интеграции сетевого и прикладного подходов (гибридный подход к НД). Посредством интерфейса SDP-контроллера в принципе можно контролировать доступ пользователей к функциям приложений на уровне сетевых соединений. Реализация программно-определяемого периметра основана на технологии авторизации одним пакетом (Single Packet Authorization, SPA) и безопасности соединений (mutal TLS, mTLS).

Существует ряд теоретических моделей, которые могут быть использованы при реализации систем НД. Наиболее общая модель авторизации описывается посредством матрицы доступа в виде кортежа (s, o, t, p), где s – субъект, o – защищаемый ресурс (объект), t – тип доступа (чтение, запись и т. п.), p – предикат, определяющий условия доступа [18]. Существуют различные варианты построения логики доступа, такие как ролевой контроль доступа RBAC (Role-Based Access Control) и контроль доступа на основе атрибутов ABAC (Attribute-Based Access Control). В настоящее время разрабатываются динамические модели авторизации, направленные на риск-ориентированный подход информационной безопасности [19].

Классическая модель контроля доступа UCON [20] может быть использована для описания реализации непрерывного контроля доступа. Наиболее близкими к НД моделями применения политик (Enforcing Policy) являются концепции ссылочного монитора (Reference Monitor), взятого из теории операционных систем, и прикладного межсетевого экрана (Application Firewall), описывающего программного посредника, который функционирует на прикладном уровне [21].

Ключевые проблемы реализации архитектуры нулевого доверия. Современная модель контроля доступа в АНД (рис. 1) описывает взаимодействие между субъектами (пользователями, компьютерными системами, программным обеспечением) и ресурсами (компьютерными системами, приложениями или данными) [1]. Доступ предоставляется посредством точки применения политики (шлюза), взаимодействующей с точкой принятия решения и защищающей ресурс и данные: система НД должна убедиться в подлинности субъекта и валидности доступа [22].

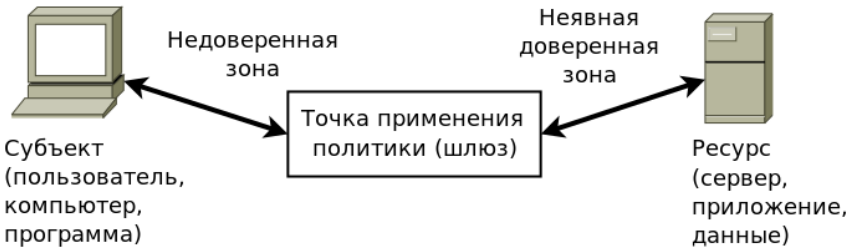

Рис. 1. Абстрактная модель контроля доступа АНД

Fig. 1. ZTA access control abstract model

НД, во-первых, ориентировано на расширение функций аутентификации и авторизации. Только авторизованный субъект сможет выполнить запрос, но при этом должны оцениваться различные параметры, например тип используемого устройства: корпоративная рабочая станция или личный мобильный телефон; наличие антивирусного программного обеспечения и последних обновлений приложений и операционной системы и т. п. Во-вторых, система защиты предназначена для обеспечения корпоративных политик безопасности: каждый запрос субъекта к ресурсу должен быть оценен на соответствие политикам. В-третьих, подчеркивается динамический аспект, т. е. корпоративные политики безопасности должны быть адаптированы к текущим рискам. Оценка безопасности доступа к ресурсам должна быть непрерывной и длительной. Например, если в процессе взаимодействия субъекта с ресурсом совокупность факторов, определивших решение предоставить доступ, перестала соответствовать политикам, то доступ следует прекратить.

Ввиду чрезмерной обобщенности и тенденции к следованию различающимся подходам современная АНД [1] имеет ряд особенностей, создающих препятствия для реализации полноценного контроля доступа. В частности, следует отметить следующие аспекты:

1. АНД представлена не как единая архитектура, а как набор принципов, архитектурных решений и операций, которые могут быть использованы для улучшения защищенности компьютерных систем предприятия [1]. Реализация АНД подразумевает применение решений разных производителей, отличающихся используемыми стандартами и технологиями, что делает актуальной проблему интероперабельности компонентов программно-технической системы защиты [23, 24].

2. Несмотря на декларирование НД (т. е. отсутствие доверия), описание АНД предполагает наличие неявных доверенных зон, особенно в сценариях, когда шлюз является точкой входа в среду, разделяемую несколькими ресурсами. Защиту «соседних» ресурсов от скомпрометированного ресурса следует рассматривать как отдельную проблему.

3. Описание АНД предполагает, что система защиты должна контролировать каждый удаленный запрос от субъекта к ресурсу в соответствии с политикой безопасности. Для полноценной реализации такого контроля система защиты должна «владеть» семантикой ресурса. Например, если ресурс является веб-приложением, то система должна «знать», какие заголовки HTTP-запросов соответствуют транзакциям чтения или записи информации; иметь перечень пользователей (групп) с описанием их прав, а также «понимать» логику реализации прав. Разработка методик и алгоритмов формализации и трансляции высокоуровневых корпоративных политик безопасности в правила конечных программно-технических систем защиты (например, листы контроля доступа или правила фильтрации контента) является важной научно-практической задачей [25].

4. Актуальной становится проблема снижения производительности информационных систем вследствие внедрения АНД. Реализация НД требует выполнения дополнительных программных процедур и проверок при взаимодействии субъектов с ресурсами. Добавление промежуточного компонента в общем случае снижает скорость доступа к ресурсу. Для принятия решения о предоставлении доступа используется соответствующий алгоритм доверия (Trust Algorithm), имеющий ненулевое время работы. Следовательно, должна быть определена необходимость применения НД к ресурсу, так как существуют корпоративные данные, которые являются публичными и не требуют авторизации. Некоторая информация не является критичной для функционирования организации. При проектировании системы защиты следует учитывать снижение скорости доступа к защищаемым ресурсам и оптимизировать параметры, определяющие производительность системы [18].

5. Являясь «горячей» темой в области информационных технологий, НД и АНД провоцируют производителей средств информационной безопасности и поставщиков облачных сервисов декларировать применение якобы передовых технологий [26] в своих продуктах без подтверждения в виде описания предлагаемых алгоритмов и функциональных возможностей. В некоторых случаях используется подмена понятий: несвязанный набор решений выдается за воплощение цельной АНД, а известные функции продуктов, реализованные ранее, рассматриваются как инновации, обеспечиваемые НД.

Принципы построения систем нулевого доверия. По сути, являясь компиляцией существующих методов обеспечения информационной безопасности, концепция НД может быть интерпретирована посредством набора известных принципов [27, 28]. Следует отметить, что принципы определяют высокоуровневые требования к архитектуре и возможные абстрактные шаблоны проектных решений. Дальнейшая детализация архитектуры может быть выполнена посредством конкретных шаблонов проектирования.

В настоящей работе предлагается интерпретировать НД как неявную (подразумеваемую) доверенную зону. Идея подобного представления не является новой. Например, в теории операционных систем известен термин «доверенная вычислительная база» (Trusted Computing Base, TCB), который ссылается на критически важные программные и аппаратные компоненты компьютерной системы, образующие безопасную среду выполнения программ. Чем компактнее доверенная вычислительная база, тем безопаснее система, так как если один компонент доверенной вычислительной базы скомпрометирован, то безопасность системы может быть нару-

шена [29]. Неявная доверенная зона служит аналогом доверенной вычислительной базы для сетевых взаимодействий и представляет собой окружение информационного ресурса, минимизирующее периметр и ограничивающее доступ к ресурсу.

Ключевыми принципами, описывающими НД, являются:

Запрещено все, что не разрешено (Deny All). Согласно данному принципу необходимо явное разрешение на публикацию ресурса и доступ к нему, т. е. по умолчанию все ресурсы недоступны. Например, утверждение «все запрещено» является вариантом правила по умолчанию в цепочке правил межсетевого экрана: если не нашлось разрешающего правила, то доступ запрещен. Альтернативой выступает правило по умолчанию «все разрешено», которое принципиально предоставляет более низкий уровень защищенности.

Минимальные привилегии (Least Priviledge) и *минимум информации* (Need To Know). Принцип минимальных привилегий требует выдачи пользователю или процессу только минимально необходимых прав для выполнения задач. Например, администратор новостей сайта должен иметь доступ к добавлению и редактированию новостей, но не должен иметь возможность размещать статьи. Принцип минимума информации касается пользователей и подчеркивает темпоральную природу доступа. Например, чтобы в данный момент получить доступ к документу при наличии права на чтение, пользователь должен иметь временное разрешение на просмотр.

Полное посредничество (Complete Mediation). Данный принцип означает, что каждый запрос к ресурсу должен быть авторизован и проверен. В описании АНД указано, что доступ к ресурсу должен быть как можно сильнее гранулирован, т. е. целью внедрения системы НД является полное посредничество.

Непрерывный мониторинг (Continuous Monitoring). Подразумевает систематический и непрерывный мониторинг защищенности компьютерных систем организации. Применение данного принципа позволяет раньше обнаруживать проблемы, смягчать риски информационной безопасности, делая корпоративные системы более надежными и защищенными. Реализация непрерывного мониторинга требует внедрения автоматизации посредством соответствующих технологий и средств.

Безопасная передача данных (Secure Communications). Данный принцип требует обеспечения свойств конфиденциальности (Confidentiality – C), целостности (Integrity – I) и доступности информации (Availability – A), передаваемой по каналам связи. Совокупность этих трех свойств называется триадой CIA и является основополагающей моделью информационной безопасности. Для виртуальных каналов передачи обеспечение конфиденциальности и доступности передаваемой информации осуществляется посредством криптографических средств, которые способны обеспечить секретность и подлинность сообщений, а также аутентификацию участников сетевого взаимодействия. Доступность информации следует рассматривать в контексте ее обработки соответствующими компьютерными системами.

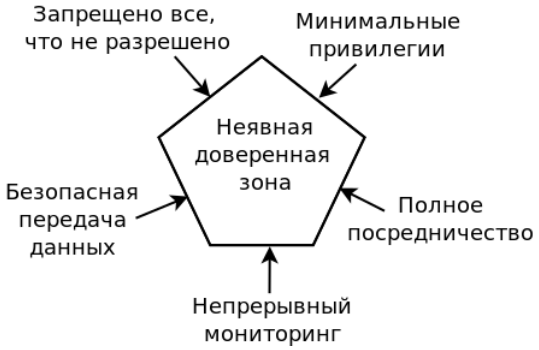

Рис. 2. Ключевые принципы АНД

Fig. 2. ZTA key principles

Таким образом, принципиально АНД можно представить как неявную доверенную зону защищаемого ресурса (группы ресурсов), в которой действуют перечисленные выше принципы (рис. 2). Следует отметить, что системы НД, решающие специфические задачи, могут дополнительно следовать другим принципам информационной безопасности [18].

Шаблон контроля доступа архитектуры нулевого доверия. Для решения повторяющихся, представленных в определенном контексте проблем проектирования компьютерных систем принято применять шаблоны (паттерны) проектирования [30]. Шаблоны проектирования разрабатываются экспертами в предметной области на основе принципов и лучших практик и используются разработчиками для создания архитектур конкретных систем [31].

Дисциплина шаблонов проектирования в зависимости от решаемых задач оперирует различными видами артефактов. Различают непосредственно шаблоны проектирования (Design Patterns) и архитектурные шаблоны (Architecture Patterns), которые ориентированы на разработку программного обеспечения [32, 33], шаблоны угроз (атак) (Threat/Attack Patterns) [34] и шаблоны безопасности (Security Patterns) [21], описывающие возможные проблемы безопасности компьютерных систем и сетей, а также способы их решения, представленные как фрагменты архитектур систем, эталонные архитектуры (Reference Architecture, RA) и эталонные архитектуры безопасности (Security Reference Architecture, SRA) [21].

Для представления шаблонов проектирования могут применяться документы в свободной форме [35]. Также существует формат представления POSA (Pattern Oriented Software Architecture), основанный на стандартных разделах, ключевыми из которых являются «Намерение» (Intent), «Контекст» (Context), «Проблема» (Problem), «Решение» (Solution), «Структура решения» (Structure of Solution), «Динамика решения» (Dynamics of Solution), «Известные реализации» (Known Uses) и «Результаты» (Consequences). Разделы, посвященные структуре и динамике решения, принято представлять в виде диаграмм UML, в частности диаграмм классов, деятельности и последовательности. Вышеназванные ключевые разделы формата POSA использованы для описания разработанного шаблона.

Представленный в настоящей работе шаблон контроля доступа АНД является производным от абстрактного шаблона контроля доступа НД [36] и расширяет последний в части проблемы проектирования, принципов обеспечения информационной безопасности и уровней контроля доступа.

Намерение. Заключается в разработке шаблона контроля доступа, описывающего общий механизм контроля удаленного доступа субъектов к ресурсам в соответствии с принципами АНД (шаблон контроля доступа АНД).

Контекст. В качестве контекста выступает организация, владеющая комплексной и гетерогенной инфраструктурой информационных технологий (ИТ). Инфраструктура ИТ может включать системы интернета вещей и киберфизические системы, использовать облачные сервисы, а также следовать таким операционным трендам, как применение собственных устройств и удаленной работы. Подобная инфраструктура характеризуется наличием распределенных сервисов, использующих данные из различных источников, и обработкой запросов от авторизованных локальных и удаленных пользователей, работающих на различных устройствах (смартфонах, личных компьютерах, рабочих станциях), а также подразумевает анонимный доступ из сети Интернет. Перечисленные выше особенности существенно увеличивают поверхность атак (attack surface) на инфраструктуру ИТ-организации.

Проблема. Включает две составляющие: проблему проектирования и практическую проблему.

Проблема проектирования заключается в том, что существующие описания АНД [1–3] являются слишком общими и содержат нечеткие и противоречивые рекомендации по реализации. Необходим шаблон проектирования, описывающий контроль доступа в рамках АНД, который мог бы использоваться для разработки архитектур конечных систем защиты и других шаблонов проектирования.

Практическая проблема связана с тем, что большинство организаций, владеющих распределенной и гетерогенной инфраструктурой ИТ, используют для обеспечения информационной

безопасности подход на основе сетевого периметра, который не соответствует множественности вариантов доступа субъектов к ресурсам и распределенному характеру ресурсов и данных организации.

Пример сценария, описывающего практическую проблему, может быть следующим [36]. Компания перенесла в публичную облачную среду несколько приложений, которые ранее были размещены в корпоративной сети, защищенной межсетевым экраном. Приложения, помещенные в сеть Интернет, характеризуемую широким анонимным доступом, стали источниками ряда инцидентов информационной безопасности. Некоторое требовательное к вычислительным ресурсам приложение является целью атаки, суть которой заключается в отправке большого количества запросов посредством сети ботов (botnet), что негативно влияет на доступность приложения и увеличивает стоимость его размещения в облаке. Данные факторы соответствуют комбинированной атаке «распределенный отказ в обслуживании» (Distibuted Denial of Service, DDoS) и «экономический отказ в обслуживании» (Economic Denial of Sustainability, EDoS). В настоящее время компания ищет способ защитить свои облачные приложения от анонимного доступа из сети Интернет и обеспечить безопасный доступ сотрудников к корпоративным приложениям независимо от расположения пользователей (офис, удаленная работа) и сервисов (корпоративная сеть, публичное облако).

Решение. Заключается в том, что промежуточный компонент должен перехватывать каждую попытку удаленного доступа субъекта к ресурсу (принцип полного посредничества), аутентифицировать субъект и предоставлять доступ, если он легитимен (соответствует политике безопасности согласно принципам «запрещено все, что не разрешено» и минимальных привилегий). При этом должна быть обеспечена безопасная передача данных между субъектом и ресурсом. Каждый акт доступа должен периодически оцениваться на легитимность и в случае нарушения политики безопасности прерываться (непрерывный мониторинг).

Структура решения. Для описания структуры решения использованы терминология и компоненты расширяемого языка разметки контроля доступа XACML (eXtensible Access Control Markup Language) [1, 21]. На рис. 3 показана диаграмма классов, описывающая структуру решения.

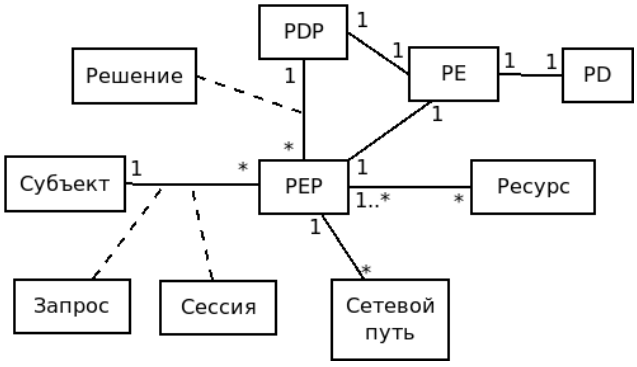

Рис. 3. Структура решения

Fig. 3. Structure of solution

Непосредственно промежуточным компонентом между субъектом и ресурсом является точка применения политики PEP (Policy Enforcement Point), которая использует решения предоставить или отклонить доступ, вырабатываемые точкой принятия решений PDP (Policy Decision Point). Компонент точки принятия решений использует систему управления политиками PE (Policy Engine), которая оперирует идентификационной информацией субъектов и компилирует политики разного уровня для авторизации субъекта и поддержки принятия решений о доступе. Для хранения корпоративных политик в машиночитаемом виде используется база данных политик PD (Policy Database).

После получения положительного решения компонент точки применения политики должен обеспечить доступ субъекта к ресурсу и безопасную передачу данных. В рамках современных представлений об АНД и сетевых технологиях контроль доступа может осуществляться на следующих уровнях:

1. Сетевой путь (Communication Path). Обязательный компонент, обеспечивающий для удаленных субъектов доступность компьютерной системы, на которой расположен ресурс. Для создания сетевого пути могут использоваться устройства и программное обеспечение, пересылающие сетевые пакеты на основе соответствующих таблиц, содержащих физические (логические) адреса и другие параметры пакетов, а также фильтрующие пакеты на основе соответствующих правил.

2. Соединение (Session). Представляет собой логическую ассоциацию между двумя удаленными программными процессами (приложениями), обеспечивающую двунаправленную передачу данных между ними. Предполагает уровень контроля доступа выше, чем сетевой путь. Примером соединения является сессия по протоколу TCP между приложением-клиентом и приложением-сервером.

3. Запрос/транзакция (Request/Transaction). Атомарный компонент, обеспечивающий наивысший уровень контроля доступа субъектов к ресурсам (полное посредничество) при условии, что семантика конкретного приложения (формат запросов, пользователи и группы, логика выдачи прав) «понятна» системе защиты, т. е. описана в терминологии корпоративных политик безопасности. Представляет собой сообщение прикладного протокола, содержащее запрос на получение или изменение данных. Примером такого сообщения может быть HTTP-запрос к веб-приложению, содержащий в заголовке указание на изменение данных, а в теле – изменяемые данные.

Динамика решения. В зависимости от используемого уровня контроля доступа в производных шаблонах и конечных АНД могут быть реализованы различные сценарии. Для сетевого пути это могут быть сценарии «Создать сетевой путь», «Мониторить сетевой путь», «Удалить сетевой путь», для соединений, например, – сценарии «Создать соединение», «Мониторить соединение», «Удалить соединение».

На рис. 4 показана схема последовательности сценария «Обработать запрос», используемого для контроля доступа на уровне запросов. Предполагается, во-первых, что запрос является атомарным действием в рамках системы защиты и не требует длительного мониторинга в отличие, например, от соединений; во-вторых, для обработки запроса сетевой путь и соединение должны существовать; в-третьих, субъект предварительно аутентифицирован в рамках другого сценария.

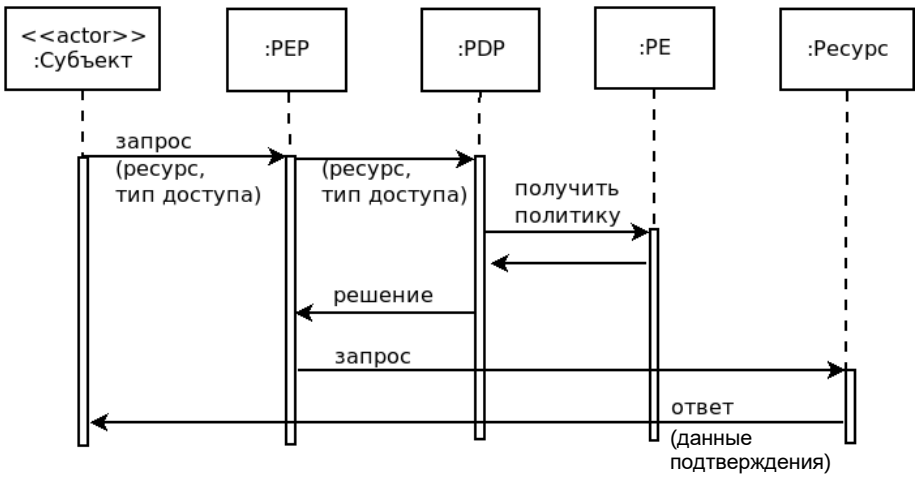

Рис. 4. Сценарий «Обработать запрос»
Fig. 4. "Process request" use case

Субъект отправляет компоненту точки применения политики запрос (рис. 4), содержащий непосредственно данные, информацию о запрашиваемом ресурсе и типе доступа (чтение, запись и т. п.). Компонент точки применения политики отправляет метаданные о запросе компоненту точки принятия решений. Компонент точки принятия решений, используя политики, предоставленные компонентом управления политиками, принимает решение относительно открытия доступа. Получив положительное решение от точки принятия решений, компонент точки применения политики передает данные запроса ресурсу для обработки.

Известные реализации. Комплексные системы виртуализации компьютерных сетей, например VMWare ESX, способны реализовать контроль доступа на уровне сетевого пути [18]. Программно-определяемый периметр обеспечивает контроль доступа и защиту передаваемых данных на уровне сетевых соединений [17]. Пилотный проект BeyondCorp компании Google является примером реализации контроля доступа на уровне сообщений прикладных протоколов [16].

Результаты. Разработанный шаблон описывает посредничество при взаимодействии субъекта с ресурсом, направленное на повышение защищенности ресурса. При использовании сценария «Обработать запрос» каждый запрос (транзакция) к ресурсу является авторизованным и валидным. При этом субъект получает минимальные права, соответствующие своим задачам. Неавторизованный доступ к ресурсам становится невозможным.

Заключение. Статья посвящена анализу теоретических и практических аспектов проектирования компьютерных систем на основе АНД. В ней сформулированы основные проблемы реализации систем НД, включая интероперабельность компонентов программно-технической системы защиты, необходимость защиты соседних ресурсов друг от друга, трансляцию корпоративных политик безопасности в правила конкретных средств защиты, снижение производительности информационных систем вследствие внедрения АНД, произвольную трактовку концепций НД и АНД производителями средств защиты.

Предложено принципиально интерпретировать АНД как неявную доверенную зону, соответствующую принципам «запрещено все, что не разрешено», минимальных привилегий, полного посредничества, непрерывного мониторинга и безопасной передачи данных.

Представлен шаблон проектирования контроля доступа АНД, который в отличие от существующих разработок описывает проблему проектирования, основан на известных принципах обеспечения информационной безопасности и учитывает возможные уровни контроля доступа.

Полученные результаты могут быть использованы для формализации абстрактных шаблонов проектирования и разработки производных шаблонов и конечных архитектур компьютерных систем на основе концепции НД.

Список использованных источников

1. Zero Trust Architecture. Special Publication (NIST SP-800-207) / S. Rose, O. Borchert, S. Mitchell, S. Connelly. – Gaithersburg : National Institute of Standards and Technology, 2020. – 59 p.

2. Kindervag, J. Build security into your network's DNA: The zero trust network architecture / J. Kindervag // Forrester Research Inc. – 2010. – 27 p. – URL: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (date of access: 14.05.2024).

3. Riley, S. Market guide for ZTNA / S. Riley, N. MacDonald // Gartner. – 2020. – URL: https://www.gartner.com/en/documents/3986053 (date of access: 14.05.2024).

4. Cunningham, C. The zero trust eXtended (ZTX) ecosystem / C. Cunningham // Forrester. – Cambridge, MA, 2018. – 15 p. – URL: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf (date of access: 14.05.2024).

5. Кучер, В. А. Микросегментация в информационной безопасности / В. А. Кучер // Молодой исследователь Дона. – 2021. – № 3. – С. 54–56.

6. Мурадова, А. А. Надежность и безопасность интернета вещей / А. А. Мурадова // SCHOLAR. – 2023. – Т. 1, № 27. – С. 109–117.

7. Использование методов искусственного интеллекта для обеспечения кибербезопасности сотовых сетей связи / Е. Сейткулов, Д. Сатыбалдина, Н. Бисенбаева [и др.] // Вестник КазАТК. – 2024. – Т. 132, № 3. – С. 319–328.

8. Набиев, Б. Р. Интеллектуальный анализ киберугроз: проблемы и перспективы / Б. Р. Набиев, К. Г. Дашдамирова // Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений : сб. материалов XVII Междунар. науч.-техн. конф., Курск, 12–15 сент. 2023 г. – Курск, 2023. – С. 166–168.

9. Assunção, P. A zero trust approach to network security / P. Assunção // Proc. of the Digital Privacy and Security Conf., Porto, Protugal, 16 Jan. 2019. – Porto, Protugal, 2019. – P. 65–72.

10. Карелова, О. Л. Сравнительный анализ межсетевых экранов нового поколения / О. Л. Карелова, Г. А. Лисин // Вестник УрФО. Безопасность в информационной сфере. – 2024. – Т. 1, № 51. – С. 22–29.

11. Глухова, Т. В. Актуальность использования SECURITY AS A SERVICE в современных реалиях / Т. В. Глухова, Е. В. Горина, О. М. Ручина // Инновации в науке. – 2015. – № 11(48). – С. 115–120.

12. Transparent microsegmentation in smart home {IoT} networks / A. Osman, A. Wasicek, S. Köpsell, T. Strufe // 3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20), Online, 25–26 June 2020. – USENIX Association, 2020. – URL: https://www.usenix.org/conference/hotedge20/presentation/osman (date of access: 14.05.2024).

13. Урбанович, П. П. Элементы современных компьютерных сетей и сетевых технологий / П. П. Урбанович, М. Д. Плонковски // Передовые технологии и материалы будущего : сб. ст. IV Междунар. науч.-техн. конф. «Минские научные чтения-2021», Минск, 9 дек. 2021 г. : в 3 т. – Минск : БГТУ, 2021. – Т. 3. – С. 240–246.

14. Нурудинов, Г. М. Адаптивное управление трафиком в SDN-сетях с применением машинного обучения / Г. М. Нурудинов // Экономика и качество систем связи. – 2024. – № 1(31). – С. 114–122.

15. Предложение стратегии новой реальности: методология нулевого доверия / А. Нурушева, Р. Сафин, А. Амренов, Д. Сатыбалдина // Вестник КазАТК. – 2023. – Т. 127, № 4. – С. 140–147.

16. Ward, R. Beyondcorp: A new approach to enterprise security / R. Ward, B. Beyer // Login: the Magazine of USENIX & SAGE. – 2014. – Vol. 39, no. 6. – P. 6–11.

17. Sallam, A. On the security of SDN: A completed secure and scalable framework using the software-defined perimeter / A. Sallam, A. Refaey, A. Shami // IEEE Access. – 2019. – Vol. 7. – P. 146577–146587.

18. Fernandez, E. B. A critical analysis of Zero Trust Architecture (ZTA) / E. B. Fernandez, A. Brazhuk // Computer Standards & Interfaces. – 2024. – Vol. 89. – P. 103832.

19. Shitov, A. Software complex for risk-oriented attribute-based access control mechanism / A. Shitov, N. Stelmakh, S. Magomedov // International Journal of Open Information Technologies. – 2024. – Vol. 12, no. 6. – P. 133–142.

20. Park, J. The UCONABC usage control model / J. Park, R. Sandhu // ACM Transactions on Information and System Security (TISSEC). – 2004. – Vol. 7, no. 1. – P. 128–174.

21. Fernandez-Buglioni, E. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns / E. Fernandez-Buglioni. – John Wiley & Sons, 2013. – 582 p.

22. 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.

23. Михневич, С. Ю. Эволюция понятия интероперабельности открытых информационных систем / С. Ю. Михневич, А. А. Тежар // Цифровая трансформация. – 2023. – Т. 29, № 2. – С. 60–66.

24. Дулин, С. К. Алгоритм улучшения согласованности структурной интероперабельности / С. К. Дулин, А. Б. Рябцев // Надежность. – 2024. – Т. 24, № 2. – С. 8–15.

25. Dang, T. K. XACs-DyPol: Towards an XACML-based Access Control Model for Dynamic Security Policy / T. K. Dang, X. S. Ha, L. K. Tran. – 2020. – URL: https://arxiv.org/abs/2005.07160 (date of access: 14.05.2024).

26. Артамонов, В. А. Искусственный интеллект и безопасность: проблемы, заблуждения, реальность и будущее / В. А. Артамонов, Е. В. Артамонова // Россия: тенденции и перспективы развития. – 2022. – Вып. 17, ч. 1. – С. 585–594.

27. Saltzer, J. H. The protection of information in computer systems / J. H. Saltzer, M. D. Schroeder // Proceedings of the IEEE. – 1975. – Vol. 63, no. 9. – P. 1278–1308.

28. Добрышин, М. М. Тенденции развития теории информационной безопасности в условиях динамического изменения парадигмы применения информационно-технических воздействий / М. М. Добрышин // Экономика и качество систем связи. – 2022. – № 1(23). – С. 37–43.

29. Способ создания доверенной аппаратно-программной платформы для применения в информационных системах специального назначения / А. Ю. Боровиков, О. А. Маслов, С. А. Мордвинов, А. А. Есафьев // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – С. 104–117.

30. Design Patterns: Elements of Reusable Object-Oriented Software / E. Gamma, R. Helm, R. Johnson, J. Vlissides. – Addison-Wesley Professional, 1994. – 416 p.

31. Валеев, С. С. Паттерны проектирования архитектуры нулевого доверия / С. С. Валеев, Н. В. Кондратьева // Инженерный вестник Дона. – 2023. – № 9. – С. 105.

32. Чернышев, С. А. Классификация общих шаблонов проектирования мультиагентных систем / С. А. Чернышев // Программные продукты и системы. – 2022. – Т. 35, № 4. – С. 670–679.

33. Ермоченко, С. А. Проектирование программного обеспечения / С. А. Ермоченко, Е. А. Корчевская. – Витебск : ВГУ имени П. М. Машерова, 2023. – 51 с.

34. Бражук, А. И. Онтологический анализ в задачах моделирования угроз системам на основе контейнерных приложений / А. И. Бражук, Е. В. Олизарович // Информатика. – 2023. – Т. 20, № 4. – С. 69–86.

35. Пасынкова, А. А. Проектирование архитектуры системы мониторинга на основе паттернов проектирования / А. А. Пасынкова, О. Л. Викентьева // Труды Института системного программирования РАН. – 2023. – Т. 35, № 3. – С. 137–150.

36. Brazhuk, A. An abstract security pattern for Zero Trust Access Control / A. Brazhuk, E. B. Fernandez // Proc. of the 29th Intern. Conf. on Pattern Languages of Programs (PLoP '22), Virtual Event, 17–24 Oct. 2022. – The Hillside Group, United States, 2022. – Article 2. – P. 1–5.

References

1. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. Special Publication (NIST SP-800-207). Gaithersburg, National Institute of Standards and Technology, 2020, 59 p.

2. Kindervag J. Build security into your network's DNA: The zero trust network architecture. *Forrester Research Inc.,* 2010, 27 p. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (accessed 14.05.2024).

3. Riley S., MacDonald N. Market guide for ZTNA. *Gartner*, 2020. Available at: https://www.gartner.com/en/documents/3986053 (accessed 14.05.2024).

4. Cunningham C. The zero trust eXtended (ZTX) ecosystem. *Forrester*, Cambridge, MA, 2018, 15 p. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf (accessed 14.05.2024).

5. Kucher V. A. *Microsegmentation in information security.* Molodoj issledovatel' Dona [*Young Explorer of the Don*], 2021, no. 3, pp. 54–56 (In Russ).

6. Muradova A. A. Reliability and security of the internet of things. *SCHOLAR*, 2023, vol. 1, no. 27, pp. 109–117 (In Russ).

7. Sejtkulov E., Satybaldina D., Bisenbaeva N., Kasenova M., Zhyzbaev S. *Using artificial intelligence methods to ensure cybersecurity of cellular networks.* Vestnik KazATK [*Bulletin of KazATC*], 2024, vol. 132, no. 3, pp. 319–328 (In Russ).

8. Nabiev B. R., Dashdamirova K. G. *Intelligent analysis of cyber threats: problems and prospects.* Optiko-jelektronnye pribory i ustrojstva v sistemah raspoznavanija obrazov i obrabotki izobrazhenij : sbornik materialov XVII Mezhdunarodnoj nauchno-tehnicheskoj konferencii, Kursk, 12–15 sentjabrja 2023 g. [*Optical-electronic Devices and Apparatuses in Pattern Recognition and Image Processing Systems : Collection of Materials of the XVII International Scientific and Technical Conference, Kursk, 12–15 September 2023*]. Kursk, 2023, pp. 166–168 (In Russ).

9. Assunção P. A zero trust approach to network security. *Proceedings of the Digital Privacy and Security Conference, Porto, Protugal, 16 January 2019.* Porto Protugal, 2019, pp. 65–72.

10. Karelova O. L., Lisin G. A. *Comparative analysis of new generation firewalls*. Vestnik UrFO. Bezopasnost' v informacionnoj sfere [*Bulletin of the Ural Federal District. Security in the Information Sphere*], 2024, vol. 1, no. 51, pp. 22–29 (In Russ).

11. Gluhova T. V., Gorina E. V., Ruchina O. M. *The relevance of using SECURITY AS A SERVICE in modern realities*. Innovacii v nauke [*Innovations in Science*], 2015, no. 11(48), pp. 115–120 (In Russ).

12. Osman A., Wasicek A., Köpsell S., Strufe T. Transparent microsegmentation in smart home {IoT} networks. *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20), Online, 25–26 June 2020*. USENIX Association, 2020. Available at: https://www.usenix.org/conference/hotedge20/presentation/osman (accessed 14.05.2024).

13. Urbanovich P. P., Plonkovski M. D. *Elements of modern computer networks and network technologies.* Peredovye tehnologii i materialy budushhego : sbornik statej IV Mezhdunarodnoj nauchno-tehnicheskoj konferencii «Minskie nauchnye chtenija-2021», Minsk, 9 dekabrja 2021 g. : v 3 tomah [*Advanced Technologies*

and Materials of the Future : Collection of Articles of the IV International Scientific and Technical Conference "Minsk Scientific Readings-2021", Minsk, 9 December 2021 : in 3 Volumes]. Minsk, Belorusskij gosudarstvennyj tehnologicheskij universitet, 2021, vol. 3, pp. 240–246 (In Russ).

14. Nurudinov G. M. *Adaptive traffic management in sdn networks using machine learning.* Ekonomika i kachestvo sistem svyazi [*Economy and Quality of Communication Systems*], 2024, no. 1(31), pp. 114–122 (In Russ).

15. Nurusheva A., Safin R., Amrenov A., Satybaldina D. *Proposing a strategy for a new reality: zero trust methodology*. Vestnik KazATK [*Bulletin of KazATC*], 2023, vol. 127, no. 4, pp. 140–147 (In Russ).

16. Ward R., Beyer B. Beyondcorp: A new approach to enterprise security. *Login: the magazine of USENIX & SAGE*, 2014, vol. 39, no. 6, pp. 6–11.

17. Sallam A., Refaey A., Shami A. On the security of SDN: A completed secure and scalable framework using the software-defined perimeter. *IEEE Access*, 2019, vol. 7, pp. 146577–146587.

18. Fernandez E. B., Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, 2024, vol. 89, p. 103832

19. Shitov A., Stelmakh N., Magomedov S. Software complex for risk-oriented attribute-based access control mechanism. *International Journal of Open Information Technologies*, 2024, vol. 12, no. 6, pp. 133–142.

20. Park J., Sandhu R. The UCONABC usage control model. *ACM Transactions on Information and System Security (TISSEC)*, 2004, vol. 7, no. 1, pp. 128–174.

21. Fernandez-Buglioni E. *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*. John Wiley & Sons, 2013, 582 p.

22. Ivanov P. A., Kapger I. V., Shaburov A. S. *Model for implementing access control to information assets in the zero trust concept*. Vestnik Permskogo nacional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [*Perm National Research Polytechnic University Bulletin. Electrotechnics, Information Technologies, Control Systems*], 2023, no. 45, pp. 147–163 (In Russ).

23. Mihnevich S. Yu., Tezhar A. A. *Evolution of the concept of interoperability of open information systems*. Cifrovaya transformaciya [*Digital Transformation*], 2023, vol. 29, no. 2, pp. 60–66 (In Russ).

24. Dulin S. K., Ryabcev A. B. *Algorithm for improving structural interoperability consistency*. Nadezhnost' [*Reliability*], 2024, vol. 24, no. 2, pp. 8–15 (In Russ).

25. Dang T. K., Ha X. S., Tran L. K. *XACs-DyPol: Towards an XACML-based Access Control Model for Dynamic Security Policy*, 2020. Available at: https://arxiv.org/abs/2005.07160 (accessed 14.05.2024).

26. Artamonov V. A., Artamonova E. V. *Artificial intelligence and security: problems, misconceptions, reality and future*. Rossiya: tendencii i perspektivy razvitiya [*Russia: Development Trends and Prospects*], 2022, iss. 17, part 1, pp. 585–594 (In Russ).

27. Saltzer J. H., Schroeder M. D. The protection of information in computer systems. *Proceedings of the IEEE*, 1975, vol. 63, no. 9, pp. 1278–1308.

28. Dobryshin M. M. *Trends in the development of information security theory in the context of dynamic change in the paradigm of the use of information technology impacts*. Ekonomika i kachestvo sistem svyazi [*Economy and Quality of Communication Systems*], 2022, no. 1(23), pp. 37–43 (In Russ).

29. Borovikov A. Yu., Maslov O. A., Mordvinov S. A., Esaf'ev A. A. *Method for creating a trusted hardware and software platform for use in special-purpose information systems*. Bezopasnost' informacionnyh tekhnologij [*Information Technology Security*], 2021, vol. 28, no. 4, pp. 104–117 (In Russ).

30. Gamma E., Helm R., Johnson R., Vlissides J. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional, 1994, 416 p.

31. Valeev S. S., Kondrat'eva N. V. *Zero trust architecture design patterns*. Inzhenernyj vestnik Dona [*Engineering Bulletin of the Don*], 2023, no. 9, p. 105 (In Russ).

32. Chernyshev S. A. *Classification of common design patterns for multi-agent systems.* Programmnye produkty i sistemy [*Software Products and Systems*], 2022, vol. 35, no. 4, pp. 670–679 (In Russ).

33. Ermochenko S. A., Korchevskaya E. A. Proektirovanie programmnogo obespecheniya. *Software Design*. Vitebsk, Vitebskij gosudarstvennyj universitet imeni P. M. Masherova, 2023, 51 p. (In Russ).

34. Brazhuk A. I., Olizarovich E. V. *Ontological analysis in the problems of container applications threat modelling*. Informatika [*Informatics*], 2023, vol. 20, no. 4, pp. 69–86 (In Russ.).

35. Pasynkova A. A., Vikent'eva O. L. *Designing a monitoring system architecture based on design patterns.* Trudy Instituta sistemnogo programmirovaniya RAN [*Proceedings of the Institute of System Programming of the Russian Academy of Sciences*], 2023, vol. 35, no. 3, pp. 137–150 (In Russ).

36. Brazhuk A., Fernandez E. B. An abstract security pattern for Zero Trust Access Control. *Proceedings of the 29th International Conference on Pattern Languages of Programs (PLoP '22), Virtual Event, 17–24 October 2022*. The Hillside Group, United States, 2022, article 2, pp. 1–5.

Информация об авторах

Бражук Андрей Иосифович, магистр естественных наук, ведущий инженер-программист Информационно-аналитического центра Гродненского государственного университета имени Янки Купалы.
E-mail: brazhuk@grsu.by

Олизарович Евгений Владимирович, кандидат технических наук, доцент, начальник Информационно-аналитического центра Гродненского государственного университета имени Янки Купалы.
E-mail: e.olizarovich@grsu.by

Information about the authors

Andrei I. Brazhuk, M. Sc., Lead Software Engineer at the Information and Analytical Center, Yanka Kupala State University of Grodno.
E-mail: brazhuk@grsu.by

Evgeny V. Olizarovich, Ph. D. (Eng.), Assoc. Prof., Head of the Information and Analytical Center, Yanka Kupala State University of Grodno.
E-mail: e.olizarovich@grsu.by