РИСК-ОРИЕНТИРОВАННАЯ АТРИБУТИВНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ОРГАНИЗАЦИЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Магомедов Ш.Г.[1], Козачок А.В.[2], Тарланов А.Т.[3]

Ключевые слова: *безопасность на основе рисков, динамические модели, риск-ориентированная модель управления доступом, ИТ-инфраструктура сервисов в сфере образования, атрибуты, модели управления доступом.*

Аннотация

Цель статьи: разработка риск-ориентированной модели управления доступом, изменяющей правила доступа в зависимости от текущего уровня риска реализации угроз информационной безопасности на основе анализа ключевых процессов в ИТ-инфраструктуре и событий информационной безопасности.

Методы исследований: анализ моделей управления доступом, теоретическая формализация, моделирование.

Результат: подход показал перспективность применения по сравнению с традиционными моделями управления доступом, а результаты исследований позволили выдвинуть предложения по дальнейшему развитию данного направления.

Научная новизна: предложена риск-ориентированная атрибутивная модель управления доступом на примере сервисов системы высшего образования и разработана политика управления доступом на основе промышленного стандарта XACML, изменяющая правила доступа с учетом оценки риска в реальном времени.

DOI: 10.21681/1994-1404-2023-1-72-82

1. Введение

Изменение геополитической обстановки в последние годы привело к необходимости пересмотра не только текущих аспектов защиты информации, но и фундаментальных основ в области информационной безопасности. Одним из базовых принципов в процессе обеспечения информационной безопасности является применение политик безопасности, позволяющих реализовывать на практике технические, организационные и правовые меры по обеспечению защищенности как объектов критической информационной инфраструктуры и государственных информационных систем, так и обрабатываемой информации. Существующие подходы к управлению безопасностью основаны на применении статических или частных политик безопасности (средств защиты) на объектах критической информационной инфраструктуры, информационных системах и других объектах информатизации.

Применение статических подходов безопасности позволяет обеспечить требуемый уровень защиты от известных и существующих угроз безопасности, однако требует внесения изменений в существующую конфигурацию средств защиты при модификации или реконфигурировании технических средств объектов информатизации при существенном изменении внешних условий.

Традиционные модели управления доступом используют логику доступа к ресурсам на основе правил управления доступом. Подобный подход решает большинство проблем при разграничении доступа к объектам, однако имеет существенный недостаток, заключающийся в применении статичных, предопределенных политик безопасности, которые не гарантируют безопасность объектов доступа в изменяющихся условиях окружающей обстановки. В различных ситуациях тра-

[1] ***Магомедов Шамиль Гасангусейнович,*** *кандидат технических наук, доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0001-8560-1937.*
E-mail: magomedov_sh@mirea.ru

[2] ***Козачок Александр Васильевич,*** *доктор технических наук, доцент, профессор кафедры КБ-4 «Интеллектуальные системы информационной безопасности» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0002-6501-2008.*
E-mail: kozachok_a@mirea.ru

[3] ***Тарланов Арслан Тарланович,*** *доцент кафедры КБ-14 «Цифровые технологии обработки данных» РТУ МИРЭА, г. Москва, Российская Федерация. ORCID: 0000-0002-7508-9682.*
E-mail: tarlanov@mirea.ru

диционные модели формируют одно и то же решение по управлению доступом [1]. Подобное поведение не позволяет использовать их в качестве адаптивных методов в изменяющихся условиях.

В последние годы по всему миру часто фиксируют инциденты, связанные с утечкой конфиденциальной информации по вине внутренних нарушителей как в частных, так и в государственных учреждениях. Из-за недетерминированного поведения пользователей иногда достаточно трудно отличить легитимные запросы доступа на предоставление полномочий на основе традиционных статичных моделей управления доступом [2].

2. Исследования в области динамических моделей управления доступом

Динамические модели управления доступом используют не только политики доступа, но и параметры реального времени, которые рассчитываются во время запроса доступа и их значение определяет решение о предоставлении доступа. Доверие к источнику запросов, риск, контекст, история и операционные потребности — примеры параметров реального времени.

В работах [3, 4] предлагаются риск-ориентированные модели управления доступом к устройствам типа Internet of Things и Internet of Vehicles. Значение риска рассчитывается на основе параметров: контекст пользователя и агента, ценности ресурса, критичность действия, базы данных рисков (история рисков). На основе полученного значения риска принимается решение о предоставлении доступа к объекту.

Авторы исследования [5] отмечают недостатки дискреционных (DAC), мандатных (MAC) и ролевых моделей управления доступом (RBAC) при функционировании в экосистемах больших данных. В статье описана риск-ориентированная модель управления доступом на основе контента (RCBAC), позволяющая решить проблему утечки конфиденциальных данных по вине внутренних нарушителей за счет применения риск-ориентированной модели управления доступом авторизованных пользователей к ресурсам. Разработанная авторами модель оценивает риск на основе содержимого данных, поведения пользователя при доступе к объекту и истории доступа пользователя. Поведение пользователя, атрибуты пользователя сравниваются с атрибутами объекта доступа, учитывается также контент запрашиваемого объекта. История доступа пользователя учитывает предыдущие запросы пользователя к объектам.

В работе [6] отмечаются также недостатки существующих моделей управления доступом для облачной инфраструктуры, поскольку статические методы описания правил доступа ведут к значительным рискам нарушения информационной безопасности и не могут полностью реализовать потребности и функционал облачных сервисов. Для решения обозначенных проблем авторы предлагают динамическую риск-ориентированную модель управления доступом. Модель состоит из четырех основных блоков: обнаружение аномалий на основе правил, оценка риска на основе потока данных, комплексное принятие решений, динамическая подстройка порогового значения риска.

В работе [7] приводится описание оценки риска как комплексного свойства, состоящего из идентификации, анализа и оценки риска.

Цель идентификации риска заключается в определении событий, способных привести к потенциальной потере данных, и получении представления о причинах, способах и месте возникновения утечки данных. Идентификация риска включает риски независимо от того, находится ли их источник под контролем организации или нет, даже если источники или причины риска неочевидны.

Анализ риска определяет значения вероятности и последствия риска. Анализ рисков может быть выполнен с разной степенью детализации в зависимости от уязвимостей или инцидентов. Методология анализа риска включает в себя три подхода: качественный, количественный и их комбинацию. Обычно сначала выполняется качественный анализ: он позволяет получить первую информацию об уровне риска и оценить, действительно ли риск критичен. После этого может быть проведена более подробная количественная оценка. Качественный анализ рисков использует шкалу, которая описывает степень риска (например, информативный, низкий, средний, высокий и критический) для воздействия на бизнес и вероятности возникновения. Эта шкала может быть адаптирована к различным ситуациям и типам риска. Результат этого подхода представляется в виде строки данных (категории).

Количественный анализ риска использует числовое значение шкалы как для воздействия, так и для вероятности. Качество такого анализа зависит от качества входных данных (точности числовых значений) и достоверности используемых моделей (например, насколько они соответствуют поведению системы, корректируют данные измерений). Способ раскрытия воздействия и вероятности будет изменен в зависимости от типа риска и цели, для которой используется оценка риска. При анализе следует также учитывать неопределенность и изменчивость как влияния на бизнес, так и вероятности. Оценка риска — это процесс, используемый для сравнения результата оценки риска, достигнутого в ходе анализа, с заданными критериями риска, чтобы определить, является ли уровень риска приемлемым или нет.

Для определения риска в работе определяются 4 категории: место исходящего запроса (офис, дом, магазин, кинотеатр, аэропорт), время инициации запроса (8—16 ч., 16—22 ч., 22—6 ч., 6—8 ч.), сервис (банковский сектор, e-mail, серфинг сайтов, электронная коммерция), устройство (персональный компьютер, ноутбук, смартфон). Далее на основе веса контекста категории, веса безопасности контекста данных и фактора зависимости рассчитывается минимальный уровень безопасности объекта, который должен обеспечиваться.

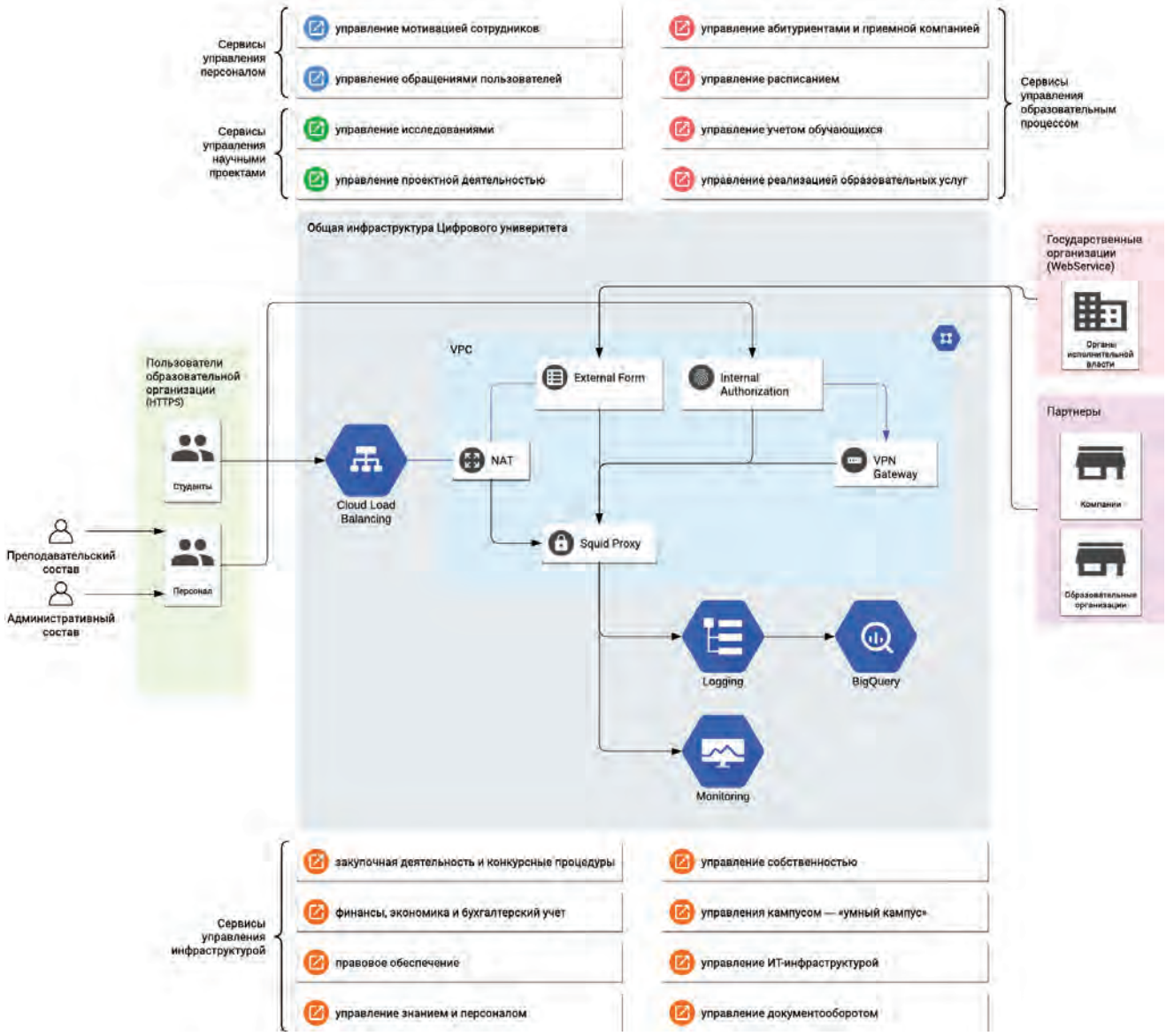

Рис. 1. Типовая структура ИТ-сервисов высшего образования

Авторы исследования [8] описывают риск-ориентированную систему управления доступом с учетом конфиденциальности для систем обнаружения угроз. Каждый запрос на доступ оценивается системой путем сравнения риска конфиденциальности и надежности запроса. Когда риск слишком велик по сравнению с уровнем доверия, фреймворк может применять стратегии адаптивной корректировки для снижения риска (например, путем выборочного запутывания данных) или для повышения уровня доверия для выполнения заданной задачи (например, наложения на пользователя обязательных к исполнению обязательств). Фреймворк может одновременно удовлетворять требованиям как конфиденциальности, так и полезности. Экспериментальные результаты, полученные авторами, показывают, что фреймворк приводит к значимым результатам и производительности в режиме реального времени в рамках решения для обнаружения промышленных угроз. Фреймворк состоит из 4 блоков: риск-ориентированный модуль контроля доступа, блок оценки риска, модуль оценки доверия запроса и модуль управления доверием и риском.

3. Управление доступом в организациях высшего образования

В современном цифровом обществе система обучения и доступа к образовательным ресурсам играет значительную роль, что было продемонстрировано с помощью анализа функционирования информационной образовательной среды в быстро меняющихся реалиях [9, 10].

Внедрение информационных технологий (ИТ) дает возможность учреждениям в сфере высшего образования усилить свои конкурентные преимущества с помощью перехода к более актуальной бизнес-стратегии, которая отвечает современным тенденциям и реализует задачи, стоящие перед образовательным учреж-

дением. С учетом последствий пандемии и различных ограничений по использованию, предлагаемых зарубежными разработчиками, образовательным учреждениям пришлось перейти на формат дистанционного обучения. Этот переход увеличил значение ИТ и, в частности, дистанционных образовательных технологий в сфере образования. Значительное число программ информатизации разработано с целью обновления ИТ-инфраструктуры учреждений образования, модернизации действующего лабораторного оснащения. Эти программы ориентированы на глобальную информатизацию, которая способствовала бы эффективному управлению организацией, предоставлению учащимся образовательных услуг, в т. ч. с использованием дистанционных технологий. Это определенным образом влияет на деятельность организаций: ИТ-инфраструктура образовательного учреждения должна быть безопасной, актуальной и масштабируемой. Именно эти требования служат основой для разработки, реализации и функционирования информационных систем в образовании.

ИТ-инфраструктурой образовательного учреждения называется совокупность программных, аппаратных, телекоммуникационных продуктов и ресурсов, необходимых для организации и реализации образовательного процесса (рис. 1).

К ИТ-инфраструктуре образовательного учреждения предъявляются следующие требования: обеспечение управления правами доступа всех пользователей, т. е. должен быть разграничен доступ пользователей к информационным ресурсам организации на основе правил, заданных в информационной системе, и должен выполняться контроль соблюдения этих правил.

В схему ИТ-инфраструктуры входят: 1) модели управления доступом (мандатные, дискреционные, ролевые); 2) виды доступа (просмотр, внесение изменений, создание, удаление, выполнение); 3) правила разграничения доступа, которые могут иметь привязку к ролям, спискам, значениям атрибутов, меткам безопасности и др.

Каждая из классических моделей управления доступом обладает своими преимуществами и недостатками, наиболее распространенной (по причине доступности и простоты реализации) является ролевая модель управления доступом (англ. role-based access control, RBAC). Суть подхода заключается в создании ролей, описывающих полномочия пользователей в соответствии с их должностными обязанностями. На основе ролей проводится проверка возможности выполнения того или иного действия пользователем.

Если иерархия ролей задана согласно штатному расписанию (преподаватель, администратор, студент и др.), то такой подход можно применять. Одной должности ставится в соответствие одна роль. Однако с увеличением сервисов, появлением новых кампусов, добавлением новых филиалов ролевая структура усложняется и становится многомерной, что влечет за собой создание новых ролей, которые будут соответствовать комбинациям всех атрибутов. Последствием этого является большое количество ролей, размытие регламента, а также сложности управления из-за отсутствия четкой иерархии.

Из этого следует, что как только для регламентов необходим контроль данных или они становятся многомерными, ролевая модель становится не только бесполезной для текущих проблем контроля доступа, но даже способствует появлению новых проблем.

Для решения проблем ролевого управления доступом был разработан другой подход, основанный на атрибутах (англ. attribute-based access control, ABAC) [11].

Главное отличие этого подхода — то, что отдельная ситуация оценивается не с позиции роли пользователя и действия, которые он планирует выполнить, а с точки зрения относящихся к ним атрибутов. Регламент — это набор условий, где разные атрибуты должны соответствовать требованиям, предъявляемым к ним для предоставления доступа.

4. Атрибутивная модель управления доступом в организациях высшего образования

Проанализировав ролевую модель управления доступом, можно сделать вывод, что данная модель подходит только для реализации простых регламентов. С ростом сложности снижается целесообразность применения ролевой модели управления доступом, потому что стоимость поддержки системы контроля доступа заметно увеличивается. При достаточно высоком уровне сложности правил применение данного подхода нецелесообразно.

Атрибутивная модель управления доступом не ограничивает сложность процессов. Из-за более простой реализации в рамках применения этого подхода стоимость поддержки при реализации более сложных правил не увеличивается. Кроме того, появляется возможность обеспечения контроля доступа и к действиям, и к данным. Данная модель является набором условий, в которых атрибуты должны соответствовать требованиям, предъявляемым к ним. Можно явно выделить несколько категорий атрибутов:

- атрибуты ресурса (тип, создатель, стоимость, название и др.);
- атрибуты субъекта (имя, отдел, должность, лимит утверждений и др.);
- атрибуты действия (название);
- атрибуты среды (IP-адрес, время, устройство).

Для того чтобы выполнить авторизацию, сравнивают значения всех атрибутов в момент проверки прав и ожидаемые значения. Доступ к ресурсу обеспечивается при выполнении всех условий.

Спроектируем ИТ-инфраструктуру образовательного учреждения с применением атрибутивной модели управления доступом.

Инфраструктура образовательного учреждения включает в себя значительное число связанных между

собой элементов, безопасность которых необходимо обеспечить:

- сервисы управления образовательным процессом;
- сервисы управления научными проектами;
- сервисы управления персоналом;
- сервисы контроля и управления доступом;
- сервисы бухгалтерского учета;
- сервисы управления инфраструктурой и др.

Среди угроз ИТ-инфраструктуре организации, работающей в сфере образования, можно назвать рассылку сообщений с вредоносными вложениями, попытки несанкционированного доступа к данным организации и многие другие. Злоумышленники разрабатывают все более совершенные механизмы атаки на информационные системы организаций, в том числе образовательных учреждений. Тогда в качестве атрибутов доступа ИТ-сервисов высшего образования можно выделить следующие атрибуты:

- роль: студент, преподаватель, административный персонал, внешние сущности, руководители подразделений;
- тип устройства доступа: рабочая ПЭВМ, ноутбук, мобильное устройство;
- тип сервиса: сервисы управления образовательным процессом, научными проектами, персоналом, инфраструктурой, сервисы контроля и управления доступом, сервисы бухгалтерского учета;
- местоположение: кампус 1, кампус 2, …, кампус N, филиал;
- тип подключения: VPN, внутренняя сеть, сеть Интернет;
- действие: запись, чтение, создание, удаление.

Необходимым требованием к ИТ-инфраструктуре организации является обеспечение защиты информационной образовательной среды организации и постоянного мониторинга и верификации пользователей. При этом пользователь должен иметь возможность оставаться в сеансе доступа к информационному ресурсу в течение времени, необходимого для работы. Работы в области адаптивной безопасности [12] показали, как применять этот вид проверок на основе различных техник.

Одна из них — это «контекстно-зависимая безопасность».

Этот подход опирается на контекстно-зависимую информацию, такую как геолокация, время доступа, репутация определенного IP-адреса или домена, тип используемого устройства и др., для принятия решений по предоставлению доступа. Вся эта информация, собранная и обработанная динамически, может обеспечить бóльшую защищенность и гранулярность относительно статических методов в различных областях применения. Эта концепция появляется в большинстве случаев в сценариях аутентификации и авторизации в распределенных системах, решение о предоставлении доступа может быть основано на различных процедурах или атрибутах в зависимости от контекста конкретного запроса.

Дополнительной техникой является инкрементная (интеллектуальная) безопасность.

Этот подход обычно сочетает в себе различные методы и инструменты, такие как большие данные, аналитика или управление информацией и событиями безопасности (SIEM), для обнаружения аномалий, выбросов или отклонений от стандартного поведения и принятия соответствующих мер. Инкрементальная (интеллектуальная) безопасность основана на сборе, стандартизации и анализе данных, генерируемых сетями, приложениями, базами данных, журналами и другой инфраструктурой в режиме реального времени. Эта информация оценивается и обрабатывается (с помощью машинного обучения, распознавания образов и др.) для перевода данных в удобочитаемый формат, который поддерживает принятие обоснованных решений.

5. Риск-ориентированная модель управления доступом для организаций высшего образования

Модель управления доступом на основе рисков является динамической моделью, которая функционирует в режиме реального времени и использует контекстную информацию для принятия решений о доступе к объекту. Эта модель выполняет расчет риска по каждому запросу на доступ к объекту и принимает решение динамически на основе полученного значения риска. Основная проблема, связанная с использованием этой модели, заключается в обеспечении оперативного, надежного и точного метода оценки риска, особенно в условиях отсутствия данных для количественного описания риска и оценки его воздействия.

Динамическая безопасность также включает в себя безопасность на основе рисков. Эта модель позволяет идентифицировать различные риски каждого из активов организации, расставляя приоритеты в отношении стоимости смягчения последствий, качества опыта и удобства использования, функциональности и др., что означает снижение этих рисков до приемлемого уровня. Этот подход позволяет организациям иметь дело с типичными компромиссами безопасности.

Необходимо постоянно отслеживать, измерять и оценивать риски, чтобы обеспечить адекватную безопасность, основанную на рисках. Необходимо также решить, как будут обрабатываться риски при их появлении. Эта методика может привести к эффективным и действенным результатам.

Большинство сценариев применения этого метода снова фокусируются на управлении доступом. Но есть и другие примеры в различных областях применения, таких как промышленные системы управлении или обработка данных.

Формирование ИТ-инфраструктуры вуза для продуктивной работы преподавателей, обучающихся и сотрудников невозможно без учета актуальных тенденций в сфере ИТ. На рис. 2 представлена риск-

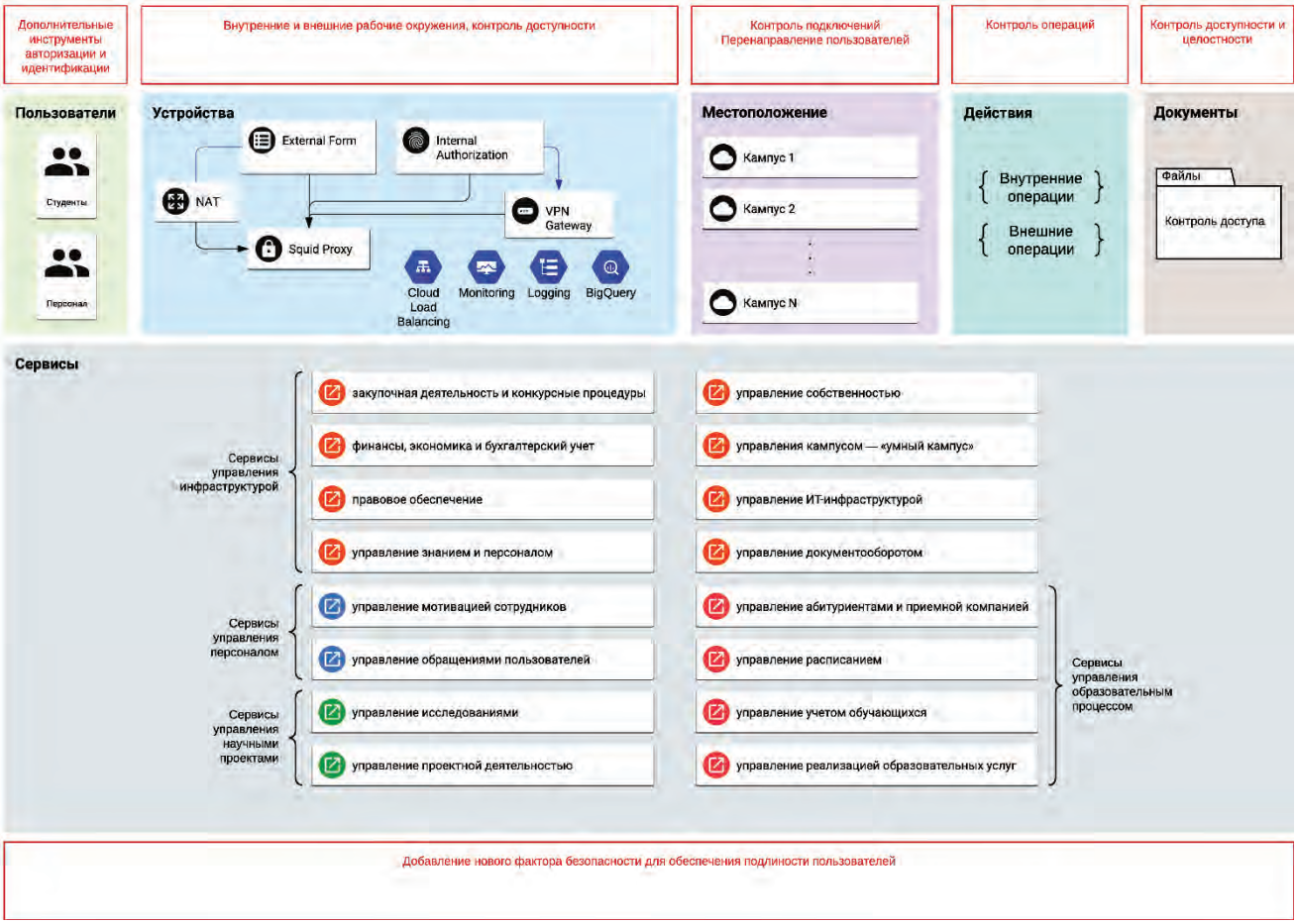

Рис. 2. Риск-ориентированная атрибутивная модель управления доступом для систем высшего образования

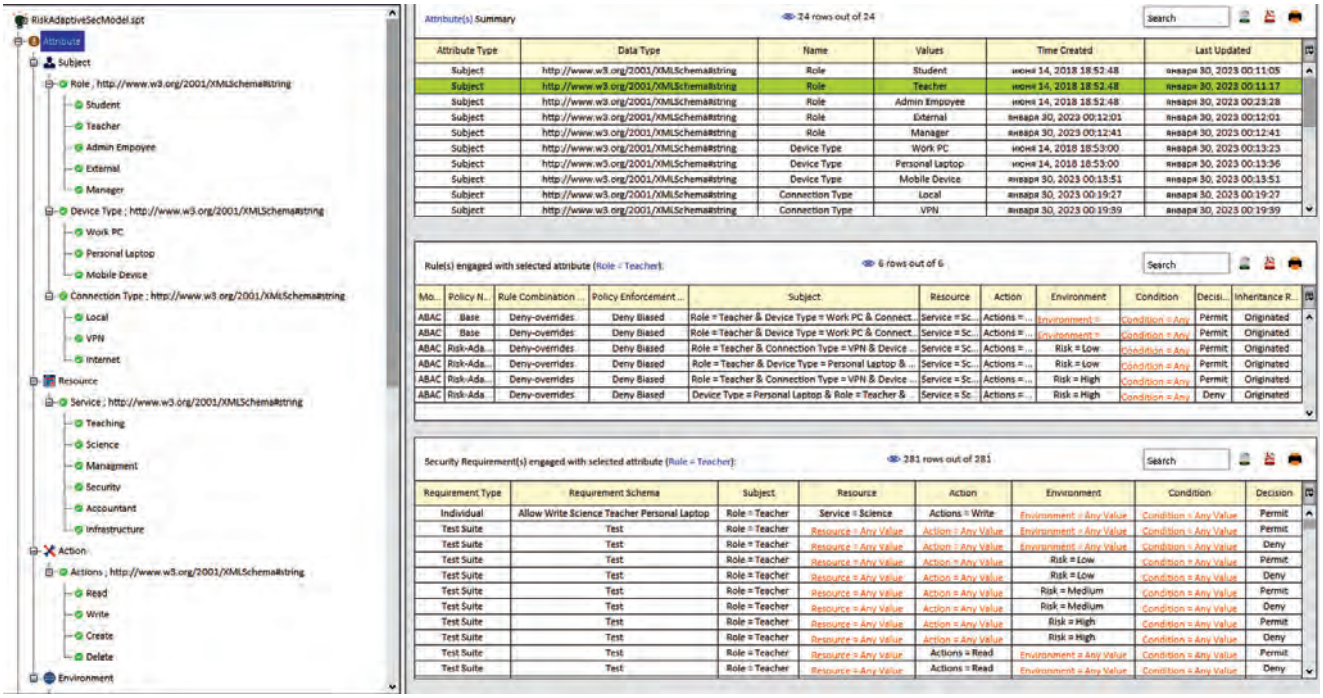

Рис. 3. Атрибуты объектов и субъектов модели

ABAC(s) Summary — 2 rows out of 2 — Search

Model	Policy Name	Rule Combination Algorithm	Policy Enforcement Algorithm	No. of Rule(s)	Time Created	L
ABAC	Base	Deny-overrides	Deny Biased	2	января 30, 2023 00:23:01	января
ABAC	Risk-Adaptive	Deny-overrides	Deny Biased	4	января 30, 2023 00:26:16	января

Rule (s) defined with selected policy (Risk-Adaptive): — 4 rows out of 4 — Search

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = Low	Condition = Any Value	Permit
2	Role = Teacher & Device Type = Personal Laptop & Connection Type = VPN	Service = Science	Actions = Write	Risk = Low	Condition = Any Value	Permit
3	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = High	Condition = Any Value	Permit
4	Device Type = Personal Laptop & Role = Teacher & Connection Type = VPN	Service = Science	Actions = Write	Risk = High	Condition = Any Value	Deny

Рис. 4. Политики атрибутивного управления доступом

ориентированная модель управления доступом для организаций высшего образования. Оценка риска реализации угроз производится на основе анализа событий безопасности в SIEM-системе и анализа поведения пользователей с учетом выбранных ранее атрибутов.

Выбор подхода к количественной оценке рисков при этом может быть обусловлен следующими факторами:

– принятая модель угроз;
– модель нарушителя;
– атрибуты безопасности управления доступом.

За основу при этом предлагается взять подход к количественной оценке рисков на основе нечетких множеств [13].

Предлагаемая модель может позволить осуществить переход от статических правил управления [14, 15] к динамически изменяемым и при этом описываемым атрибутивной моделью управления доступом. Значение риска в этом случае является дополнительным атрибутом безопасности управления доступом.

Разработка модели и ее валидация производилась в среде Security Policy Tool (URL: https://securitypolicytool.com/). Для субъектов и объектов модели были заданы соответствующие атрибуты, описанные в разделе 4 статьи (рис. 3).

Были также заданы две политики атрибутивного управления доступом, в одной из которых производился учет значения рисков, а в другой — нет (рис. 4).

В риск-ориентированной модели управления доступом при доступе преподавателя к научным сервисам с личного ноутбука при подключении VPN и высоком значении риска доступ на запись запрещен.

Для валидации корректности модели был задан инвариант безопасности, разрешающий доступ препо-

Policy Verification (января 30, 2023 00:31:53)(s) Summary — 1 rows out of 1 — Search

Status	Name	Verification T...	Verification Tech...	Number of Poli...	Combination Algo...	Enforcement Algor...	Policy List
Outdat...	Policy Verification (января 30, 2023 ...	Standard	Merged Policy	2	Deny-overrides	Deny Biased	ABAC:Base, ABAC:Risk-A...

Warning : Changes to following input parameter(s) may render previous verification result inaccurate.

Requirement Schema(s) : Allow Write Science Teacher Personal Laptop

Please Refresh Policy Verification (января 30, 2023 00:31:53)(s) to ensure recent changes are updated in your results.

Result(s) with selected verification (Policy Verification (января 30, 2023 00:31:53)) — 2 rows out of 2 — Search

Requirement Schema	Subject	Resource	Action	Environment	Condition	Decision	Verification Result
Test	Role = Teacher	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE
Test	Device Type = Personal Laptop	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE

Рис. 5. Результаты тестирования инварианта безопасности для заданных политик

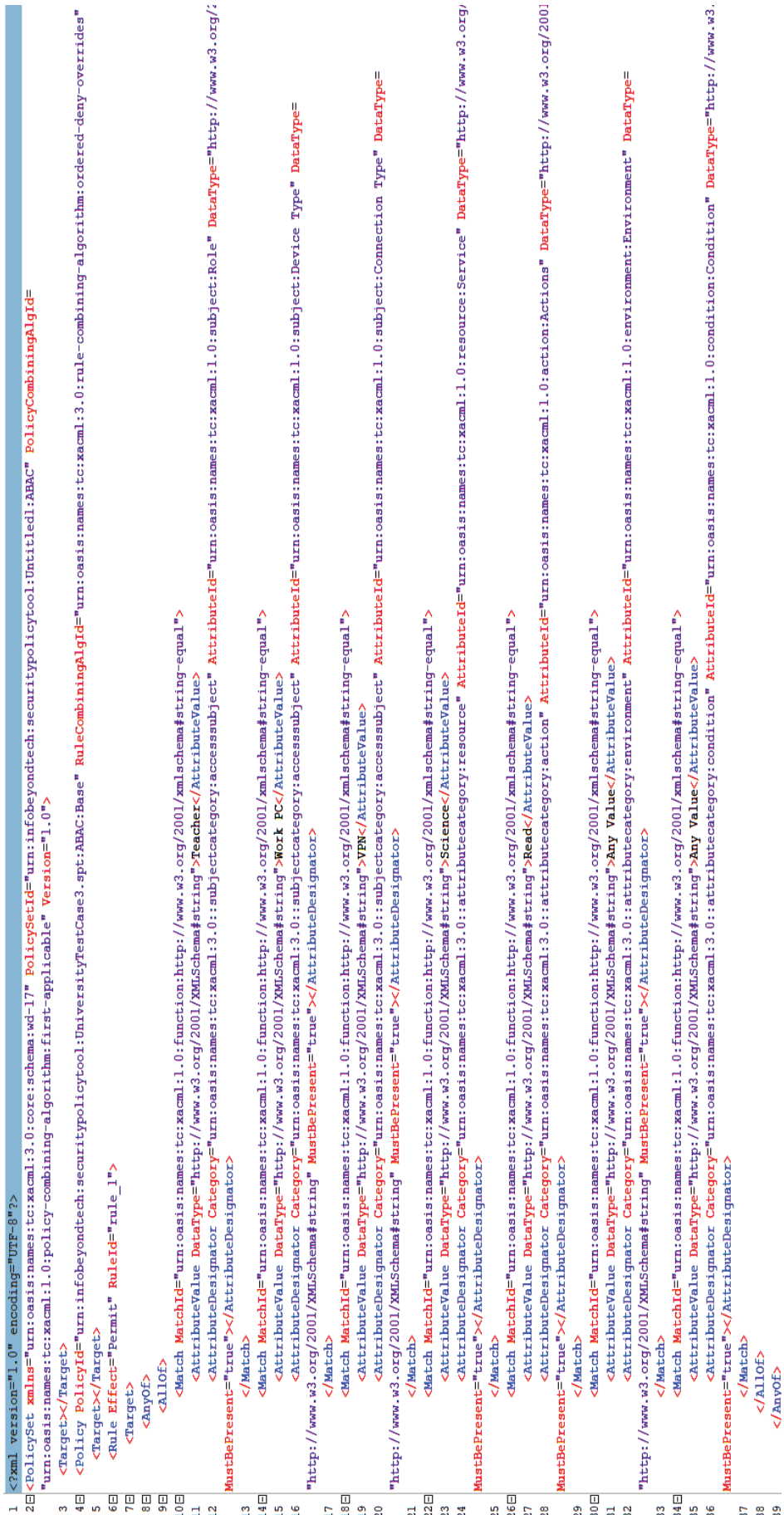

Рис. 6. Фрагмент риск-ориентированной политики управления доступом на языке XACML

давателя к научным сервисам с личного ноутбука при подключении VPN на запись. Тестирование моделей позволило выявить невыполнение данного инварианта для риск-ориентированной модели управления доступом (рис. 5).

Невыполнение указанного инварианта подтверждает корректную работу модели с учетом анализа рисков безопасности. Дополнительно была сгенерирована политика в формате XACML для обеспечения возможности использования ее в инфраструктуре образовательных организаций (рис. 6). XACML (расширяемый язык разметки управления доступом) — это открытый стандарт для авторизации и управления доступом, который обеспечивает детальный контроль над тем, кто из пользователей имеет доступ к каким ресурсам и какие действия может выполнять. Он используется для определения политик управления доступом в распределенных системах и приложениях.

6. Выводы

Предложенная риск-ориентированная модель управления доступом позволяет осуществить переход от статических правил управления доступом, используемых в классических моделях управления доступом, к динамическим, изменяющимся правилам с учетом оценки рисков реализации угроз. Оценку рисков предполагается осуществлять на основе подходов, связанных с нечеткими множествами, для определения количественной оценки рисков, что определяет область дальнейших исследований.

*Рецензент: **Алексеев Владимир Витальевич,** доктор технических наук, профессор, член-корреспондент РАЕН, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vvalex1961@mail.ru

Литература

1. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT // Mobile Networks and Applications. 2021, Vol. 26, No. 2, pp. 1—13. DOI: 10.1007/s11036-019-01214-w .
2. Ma K., Yang G., Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data // Journal of Network and Computer Applications. 2020, Vol. 167. DOI: 10.1016/j.jnca.2020.102733 .
3. Priscila S.S. et al. Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence // Security and Communication Networks. 2022, Vol. 2022. DOI: 10.1155/2022/3379843 .
4. Atlam H.F., Wills G.B. An efficient security risk estimation technique for risk-based access control model for IoT // Internet Things. 2019, Vol. 6, Article ID 100052. DOI: 10.1016/j.iot.2019.100052 .
5. Fan X., Li C., Dong X. A real-time network security visualization system based on incremental learning. // J. Visualization 22 (1), 2019, pp. 215—229.
6. Chen A., Lu G., Xing H., Xie Y., Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments // International Journal of Distributed Sensor Networks. 2020, Vol. 16. Iss. 5. DOI: 10.1177/1550147720921778 .
7. Sepczuk M., Kotulski Z. A new risk-based authentication management model oriented on user's experience // Computers & Security. 2018, Vol. 73, pp. 17—33. DOI: 10.1016/j.cose.2017.10.002 .
8. Armando A., Bezzi M., Metoui N., Sabetta A. Risk-Based Privacy-Aware Information Disclosure. In: Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. 2019, pp. 567—586. DOI: 10.4018/978-1-5225-7113-1.ch030 .
9. Магомедов Ш.Г., Колясников П.В., Никульчев Е.В. Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей // Russian Technological Journal. 2020. Т. 8. № 6 (38). С. 34—46. DOI: 10.32362/2500-316X-2020-8-6-34-46 .
10. Магомедов Ш.Г. Архитектура вычислительного комплекса с многоуровневым контролем доступа к веб-сервисам по общедоступным сетям // International Journal of Open Information Technologies. 2021. Т. 9. № 3. С. 36—43.
11. Xu Y. et al. An efficient privacy-enhanced attribute-based access control mechanism // Concurrency and Computation: Practice and Experience. 2020, Vol. 32, No. 5, p. e5556.
12. Calvo M., Beltrán M. A model for risk-based adaptive security controls // Computers & Security. 2022, Vol. 115. DOI: 10.1016/j.cose.2022.102612 .
13. Petrović Dejan V., Miloš Tanasijević, Saša Stojadinović, Jelena Ivaz, Pavle Stojković. Fuzzy Model for Risk Assessment of Machinery Failures // Symmetry. 2020. Vol. 12, No. 4, p. 525. DOI: 10.3390/sym12040525 .

14. Козачок А.В. Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем // Вопросы кибербезопасности. 2018. № 4 (28). С. 2—8. DOI: 10.21681/2311-3456-2018-4-2-8 .
15. Козачок А.В., Козачок В.И., Кочетков Е.В. Многоуровневая модель политики безопасности управления доступом операционных систем семейства Windows // Вопросы кибербезопасности. 2021. № 1 (41). С. 41—56. DOI: 10.21681/2311-3456-2021-1-41-56 .

A RISK-ORIENTED ATTRIBUTIVE ACCESS CONTROL MODEL FOR HIGHER EDUCATION ORGANISATIONS

Shamil' Magomedov, *Ph.D. (Technology), Associate Professor, Head of the Department KB-4 "Intelligent Information Security Systems" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0001-8560-1937.*
E-mail: magomedov_sh@mirea.ru

Aleksandr Kozachok, *Dr.Sc. (Technology), Associate Professor, Professor at the Department KB-4 "Intelligent Information Security Systems" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0002-6501-2008.*
E-mail: kozachok_a@mirea.ru

Arslan Tarlanov, *Associate Professor at the Department KB-14 "Digital Technologies for Data Processing" of the Russian Technological University MIREA, Moscow, Russian Federation. ORCID: 0000-0002-7508-9682.*
E-mail: tarlanov@mirea.ru

Keywords: *risk-based security, dynamic models, risk-oriented access control model, IT services infrastructure in the field of education, attributes, access control models.*

Abstract

Purpose of the paper: working out a risk-oriented access control model changing access rules in accordance with the current level of information security threat risk based on the analysis of key processes in the IT structure and information security events.

Methods of study: analysis of access control models, theoretical formalisation, simulation.

Study findings: the approach demonstrated its viability compared with traditional access control models, and the study findings made it possible to put forward proposals for further development of this research area.

Research novelty: a risk-oriented attributive access control model using the higher education system services as an example is proposed, and an access control policy based on the XACML industry standard is worked out which can change access rules according to risk assessment in real time.

References

1. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. Mobile Networks and Applications. 2021, Vol. 26, No. 2, pp. 1–13. DOI: 10.1007/s11036-019-01214-w .
2. Ma K., Yang G., Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data. Journal of Network and Computer Applications. 2020, Vol. 167. DOI: 10.1016/j.jnca.2020.102733 .
3. Priscila S.S. et al. Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence. Security and Communication Networks. 2022, Vol. 2022. DOI: 10.1155/2022/3379843 .
4. Atlam H.F., Wills G.B. An efficient security risk estimation technique for risk-based access control model for IoT. Internet Things. 2019, Vol. 6, Article ID 100052. DOI: 10.1016/j.iot.2019.100052 .
5. Fan X., Li C., Dong X. A real-time network security visualization system based on incremental learning. J. Visualization 22 (1), 2019, pp. 215–229.
6. Chen A., Lu G., Xing H., Xie Y., Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments. International Journal of Distributed Sensor Networks. 2020, Vol. 16. Iss. 5. DOI: 10.1177/1550147720921778 .

7. Sepczuk M., Kotulski Z. A new risk-based authentication management model oriented on user's experience. Computers & Security. 2018, Vol. 73, pp. 17–33. DOI: 10.1016/j.cose.2017.10.002 .
8. Armando A., Bezzi M., Metoui N., Sabetta A. Risk-Based Privacy-Aware Information Disclosure. In: Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. 2019, pp. 567–586. DOI: 10.4018/978-1-5225-7113-1.ch030 .
9. Magomedov Sh.G., Koliasnikov P.V., Nikul'chev E.V. Razrabotka tekhnologii kontrolia dostupa k tsifrovym portalam i platformam na osnove vstroennykh v interfeis otsenok vremeni reaktsii pol'zovatelei. Russian Technological Journal, 2020, t. 8, No. 6 (38), pp. 34–46. DOI: 10.32362/2500-316X-2020-8-6-34-46 .
10. Magomedov Sh.G. Arkhitektura vychislitel'nogo kompleksa s mnogourovnevym kontrolem dostupa k veb-servisam po obshchedostupnym setiam. International Journal of Open Information Technologies, 2021, t. 9, No. 3, pp. 36–43.
11. Xu Y. et al. An efficient privacy-enhanced attribute-based access control mechanism. Concurrency and Computation: Practice and Experience. 2020, Vol. 32, No. 5, p. e5556.
12. Calvo M., Beltrán M. A model for risk-based adaptive security controls. Computers & Security. 2022, Vol. 115. DOI: 10.1016/j.cose.2022.102612 .
13. Petrović Dejan V., Miloš Tanasijević, Saša Stojadinović, Jelena Ivaz, Pavle Stojković. Fuzzy Model for Risk Assessment of Machinery Failures. Symmetry. 2020. Vol. 12, No. 4, p. 525. DOI: 10.3390/sym12040525 .
14. Kozachok A.V. Cpetsifikatsiia modeli upravleniia dostupom k raznokategoriinym resursam komp'iuternykh sistem. Voprosy kiberbezopasnosti, 2018, No. 4 (28), pp. 2–8. DOI: 10.21681/2311-3456-2018-4-2-8 .
15. Kozachok A.V., Kozachok V.I., Kochetkov E.V. Mnogourovnevaia model' politiki bezopasnosti upravleniia dostupom operatsionnykh sistem semeistva Windows. Voprosy kiberbezopasnosti, 2021, No. 1 (41), pp. 41–56. DOI: 10.21681/2311-3456-2021-1-41-56 .