УПРАВЛЕНИЕ ДОСТУПОМ К ЭЛЕКТРОННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ ВУЗОВ ФЕДЕРАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Котенко И.В.[1], Саенко И.Б.[2], Захарченко Р. И.[3], Капустин А.С. [4], Аль-Барри М.Х.[5]

Цель статьи: *анализ проблемы обеспечения своевременного санкционированного доступа к ресурсам электронной информационно-образовательной среды вузов федеральных органов исполнительной власти и выявление возможных направлений ее решения.*

Методы исследования: *системный анализ проблемы обеспечения доступа должностных лиц вузов федеральных органов исполнительной власти к ресурсам электронной информационно-образовательной среды.*

Полученный результат: *предложены подходы к совершенствованию существующей модели управления доступом, оптимизации ролевой схемы доступа и идентификации попыток несанкционированного доступа на основе методов машинного обучения.*

Область применения предложенного подхода: *система управления доступом электронной информационно-образовательной среды вузов федеральных органов исполнительной власти.*

Научная новизна: *заключается в проведенном всестороннем анализе проблемы построения и функционирования электронной информационно-образовательной среды вузов федеральных органов исполнительной власти, в ходе которого определена структура этой среды и выделены ее характерные особенности. На основе анализа угроз безопасности информации в электронной информационно-образовательной среде обоснована необходимость построения системы управления доступом к ее ресурсам, обеспечивающей своевременный санкционированный доступ. Предложенные подходы к совершенствованию системы управления доступом затрагивают не только улучшение существующей модели доступа за счет ее дополнения решениями, имеющимися в атрибутивной модели, но и оптимизацию ролевой схемы доступа с помощью разработанного генетического алгоритма и обнаружение попыток несанкционированного доступа, связанных с преодолением правил доступа, основанное на применении методов машинного обучения. Приведены экспериментальные результаты, подтверждающие результативность предложенных подходов.*

Вклад: *Котенко И.В. – анализ положения дел по построению и применению электронной информационно-образовательной среды вузов федеральных органов исполнительной власти, постановка задачи и выработка предложений по развитию функциональности системы управления доступом, разработка подходов к генетической оптимизации схемы доступа и обнаружению попыток несанкционированного доступа с помощью методов машинного обучения; Саенко И.Б. – разработка подходов к совершенствованию системы управления доступом, связанных с использованием атрибутивной модели доступа, генетической оптимизации схемы доступа и обнаружения попыток несанкционированного доступа с помощью методов машинного обучения; Захарченко Р.И. – анализ технических решений, обеспечивающих реализацию системы управления доступом к ресурсам электронной информационно-образовательной среды вузов федеральных органов исполнительной власти, Капустин А.С. – анализ угроз безопасности и моделей управления доступа к ресурсам электронной информационно-образовательной среды вузов федеральных органов исполнительной власти, Аль-Барри М.Х. –*

1 Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Саенко Игорь Борисович, доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ibsaen@comsec.spb.ru

3 Захарченко Роман Иванович, доктор технических наук, начальник кафедры, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: romanzakharchenko@yandex.ru

4 Капустин Александр Сергеевич, адъюнкт, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: redbull1666@mail.com

5 Аль-Барри Мазен Хамед, адъюнкт, Военная академия связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: mazenb51@gmail.com

DOI:10.21681/2311-3456-2023-2-73-84

разработка и экспериментальное исследование подхода к обнаружению попыток несанкционированного доступа к ресурсам электронной информационно-образовательной среды вузов федеральных органов исполнительной власти, основанному на применении методов машинного обучения.

Ключевые слова: *кибербезопасность, электронная информационно-образовательная среда вузов, модель управления доступом, мандатное управление доступом, ролевое управление доступом, генетический алгоритм, машинное обучение.*

DOI:10.21681/2311-3456-2023-2-73-84

Введение

В настоящее время процесс цифровизации все более активно проникает в различные сферы жизни нашего общества, включая систему высшего образования. Тенденция к использованию документов в цифровом виде приводит к возможности реализации в высших учебных заведениях (вузах) электронного обучения, что закреплено на законодательном уровне в Федеральном законе N 273-ФЗ «Об образовании в Российской Федерации» от 21 декабря 2012 года. Одним из требований этого документа при реализации вузовских образовательных программ является создание условий для функционирования электронной информационно-образовательной среды (ЭИОС), которая включает в себя информационные технологии, технические средства, электронные информационные и электронные образовательные ресурсы. Целью создания ЭИОС является повышение доступности информационных и образовательных ресурсов, что непосредственно влечет повышение качества обучения в высшей школе. Взаимосвязь основных компонентов ЭИОС вуза представлена на рисунке 1.

В вузах федеральных органов исполнительной власти в настоящее время также происходит формирование или совершенствование ЭИОС. Вопросы построения и эффективного использования этой среды активно реализуются в вузах Министерства обороны [1-4], МВД [5,6], МЧС [7,8], Росгвардии [9,10], МИД [11] и других федеральных министерств, служб и агентств. Учитывая особенности учебного процесса в вузах федеральных органов исполнительной власти, связанные с необходимостью обеспечения информационной безопасности, остро встает проблема управления доступом к ресурсам ЭИОС. Рассмотрение подходов к ее решению, направленных на совершенствование системы управления доступом к ЭИОС, является целью настоящей работы.

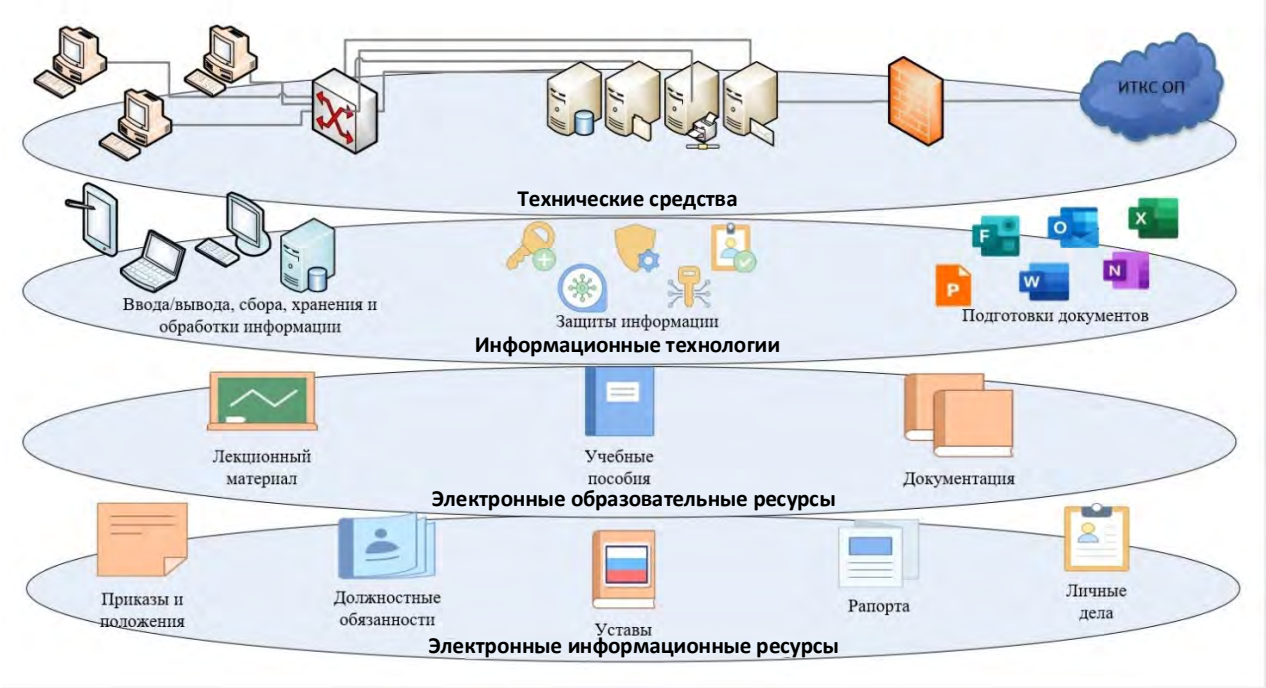

Рис. 1. Основные компоненты ЭИОС вуза

Особенности ЭИОС вузов федеральных органов исполнительной власти

Технической основой построения ЭИОС в вузах федеральных органов исполнительной власти является локальная вычислительная сеть. Вариант построения такой сети представлен на рисунке 2.

Анализируя структуру локальной вычислительной сети вуза и ее роль в построении ЭИОС, можно выделить следующие характерные особенности, присущие этой сети:

— высокая степень гетерогенности, выраженная наличием различных рабочих станций, операционных систем и приложений;
— возрастающее количество технических устройств (ноутбуки, планшеты, персональные компьютеры и др.), с которых возможна реализация доступа к ресурсам ЭИОС;
— наличие большого количества абонентов (преподаватели кафедр, слушатели и др.), реализующих доступ к информационным ресурсам ЭИОС с различных мест (учебные городки, учебные корпуса, общежития, точки свободного доступа и т.д.);
— высокая масштабируемость, обусловленная использованием различных сегментов обмена информацией, что влечет за собой обязательное применение множества как программных, так и аппаратных средств защиты информации;
— наличие объектов доступа, находящихся в зоне ответственности различных администраторов безопасности сети.

Ключевым отличием ЭОИС, развертываемых в вузах федеральных органов исполнительной власти, является многообразие информации, подлежащей защите от несанкционированного доступа, особенно при изучении специальных дисциплин [12]. При этом особое внимание, с точки зрения безопасности, уделяется информации, попадающей под категорию государственной тайны, регламентируемой. Для этого в локальной вычислительной сети реализован закрытый сегмент передачи данных с высоким уровнем доверия. Также в этих целях имеется конфиденциальный сегмент, в котором циркулирует информация служебного характера, разглашение которой за пределами вуза недопустимо. Наличие открытого сегмента обуславливается циркуляцией информации свободного распространения, не регламентируемой законодательными актами. Возможность доступа в сеть общего пользования «Интернет» из локальной вычислительной сети вуза федерального органа исполнительной власти определяется необходимостью поиска информации из открытых источников.

Таким образом, можно сделать вывод, что ЭИОС вузов федеральных органов исполнительной власти является сложной организационно-технической системой с большим количеством пользователей (среднее количество преподавателей, слушателей, руководящего состава и технического персонала превышает зачастую 2000 человек), разнообразием компьютерных средств с различными семействами и версиями

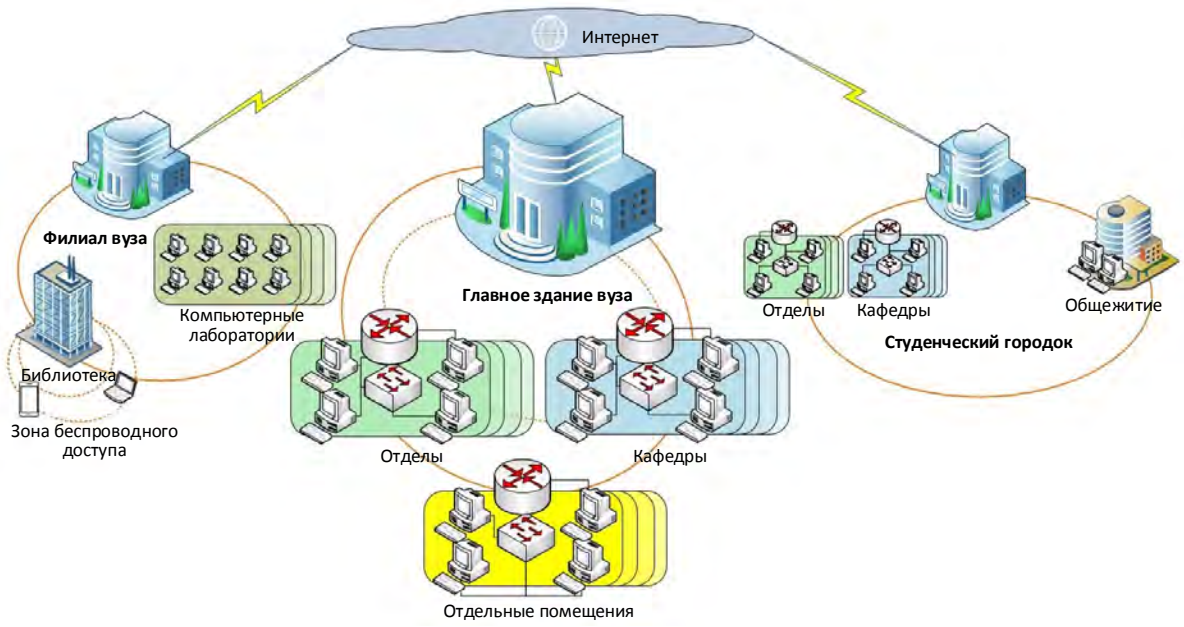

Рис. 2. Локальная вычислительная сеть вуза

операционных систем, а также наличием нескольких уровней обмена информацией. При этом необходимо подчеркнуть, что концепция ЭИОС подразумевает необходимость обеспечения индивидуального доступа вне зависимости от места нахождения пользователя. С учетом того, что в ЭИОС вузов федеральных органов исполнительной власти циркулирует информация различного рода конфиденциальности, а также существует необходимость доведения информации до ответственных лиц в части касающейся и/или в определенном временном интервале, существует необходимость в разработке рациональных решений по управлению доступом к ЭИОС.

В этой связи рассмотрим вначале понятие своевременного санкционированного доступа к ресурсам ЭИОС вуза. Санкционированный доступ – это доступ к информации, не нарушающий правила разграничения доступа. Основное правило разграничения доступа – не дать доступ к информации пользователю, который в конкретный момент времени не имеет на это права, т.е. ограничить круг лиц, имеющих доступ к этой информации, и, тем самым, сохранить ее конфиденциальность. При этом важно обеспечить доступность информации, т.е. возможность своевременного доступа субъектов (пользователей и программ) к информации в рамках имеющихся у них прав доступа. Таким образом, своевременный санкционированный доступ сводится к процессу управления в реальный момент времени доступом субъектов к объектам доступа, не нарушающему такие свойства безопасности информации, как доступность и конфиденциальность.

Согласно анализу банка данных угроз ФСТЭК, действия любого нарушителя направлены на нарушение указанных выше свойств безопасности посредствам реализации следующих угроз (рисунок 3):

- утечка информации;
- несанкционированная подмена;
- несанкционированный массовый сбор;
- несанкционированный доступ;
- удаление информационных ресурсов;
- отказ в обслуживании;
- распространение противоправной информации;
- ненадежное (нецелевое) использование;
- несанкционированная модификация (искажение);
- нарушение функционирования (работоспособности);
- получение информационных ресурсов из недоверенного или скомпрометированного источника.

Основной угрозой среди вышеперечисленных является угроза несанкционированного доступа (НСД). Для ее реализации нарушитель может применять различные методы и способы. Для недопущения реализации возможных угроз регуляторы определяют меры, позволяющие нивелировать существующие намерения нарушителя. Одной из таких мер является реализация системы управления доступом к ресурсам ЭИОС [13].

На подсистему управления доступом возлагается выполнение следующих функций:

- идентификация и проверка подлинности субъектов (пользователей ЭИОС) и объектов доступа (ресурсов ЭИОС), а также терминалов, компьютеров, узлов локальной вычислительной сети, каналов связи и прочих устройств;
- контроль доступа субъектов к защищаемым объектам доступа;
- управление потоками информации.

Задача создания системы управления доступом является многоплановой. Выделим некоторые направления в ее решении (подзадачи), для решения которых имеются наработки. Таковыми направлениями являются:

- усовершенствование модели управления доступа к ресурсам ЭИОС;
- оптимизация схемы разграничения доступа;
- обнаружение попыток НСД на основе методов машинного обучения.

Рассмотрим подходы к решению этих подзадач.

Подход к усовершенствованию модели управления доступом

Функционирование системы управления доступом опирается на выбранную модель управления доступом, которая определяет правила доступа с учетом атрибутов субъектов, объектов и среды доступа [14]. Существует множество способов управления доступом, которые описаны различными формальным моделями. Однако при этом все они нацелены на решение следующей главной задачи – формирование правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности информации в системе. Однако вопросы своевременности санкционированного доступа при этом зачастую не рассматриваются либо рассматриваются не в полной мере.

Анализируя наиболее известные и чаще всего применяемые в автоматизированных системах модели

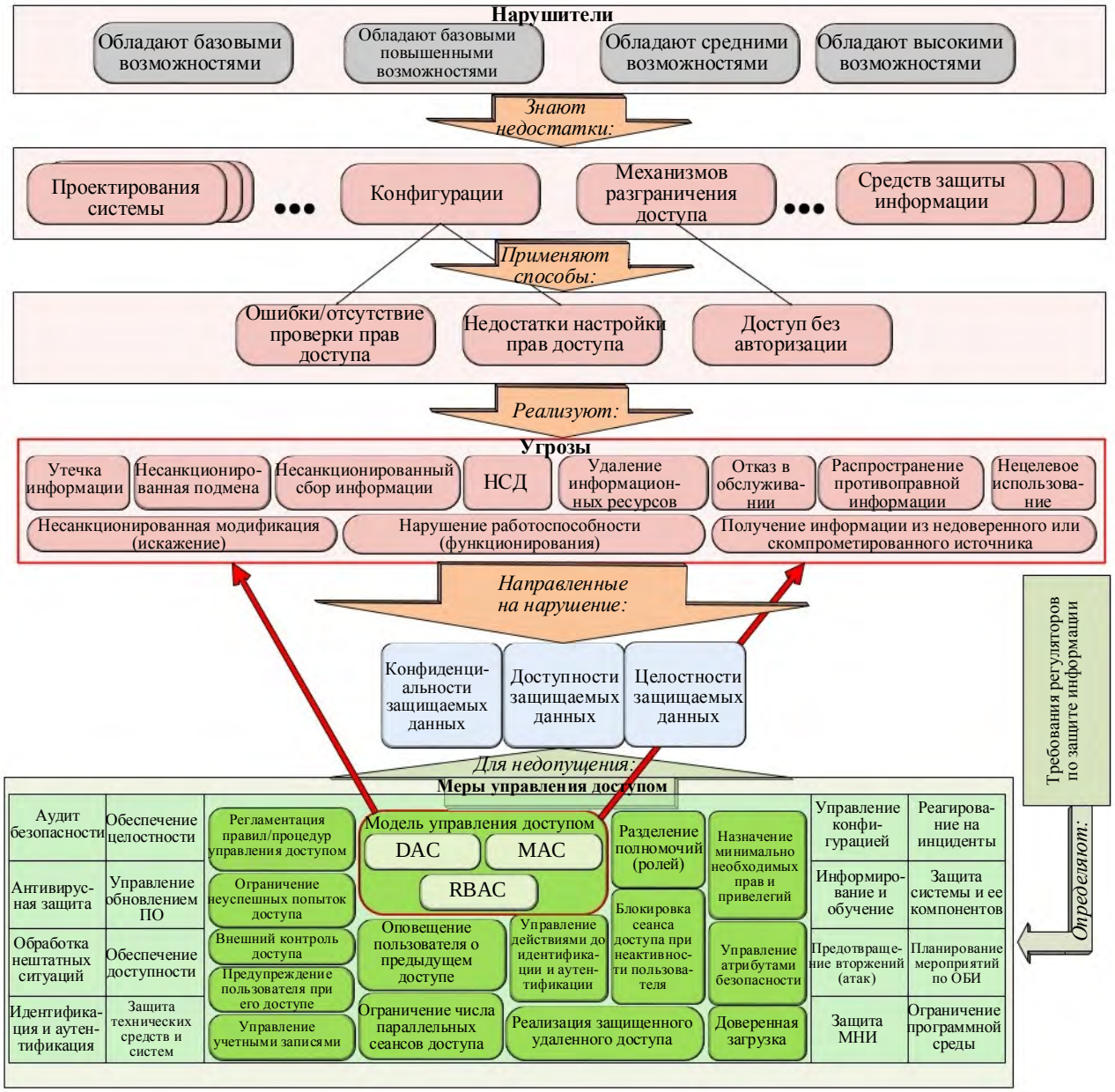

Рис. 3. Сопоставление угроз информации и мер по их недопущению

управления доступом, можно построить схему их эволюции, представленную на рис. 4.

Все эти модели успешно применяются для разграничения доступа как самостоятельно, так и в совокупности с другими моделями. Однако эти модели не в полном объеме реализуют процесс изменения прав доступа на основе модификации атрибутов в реальном моменте времени, что, соответственно, снижает эффективность управления доступом к ресурсам ЭИОС вузов федеральных органов исполнительной власти.

Наиболее предпочтительной для использования в ЭИОС вузов федеральных органов исполнительной власти является мандатная сущностно-ролевая ДП-модель (МРОСЛ-ДП модель) управления доступом, реализованная в операционной системе Astra Linux [15]. Данная модель интегрирует ролевое и мандатное управление доступом, мандатный контроль целостности, а также включает контроль информационных потоков по памяти и по времени. Однако, несмотря на достоинство данной модели, выраженное в объединении всех положительных особенностей ролевой и мандатной моделей

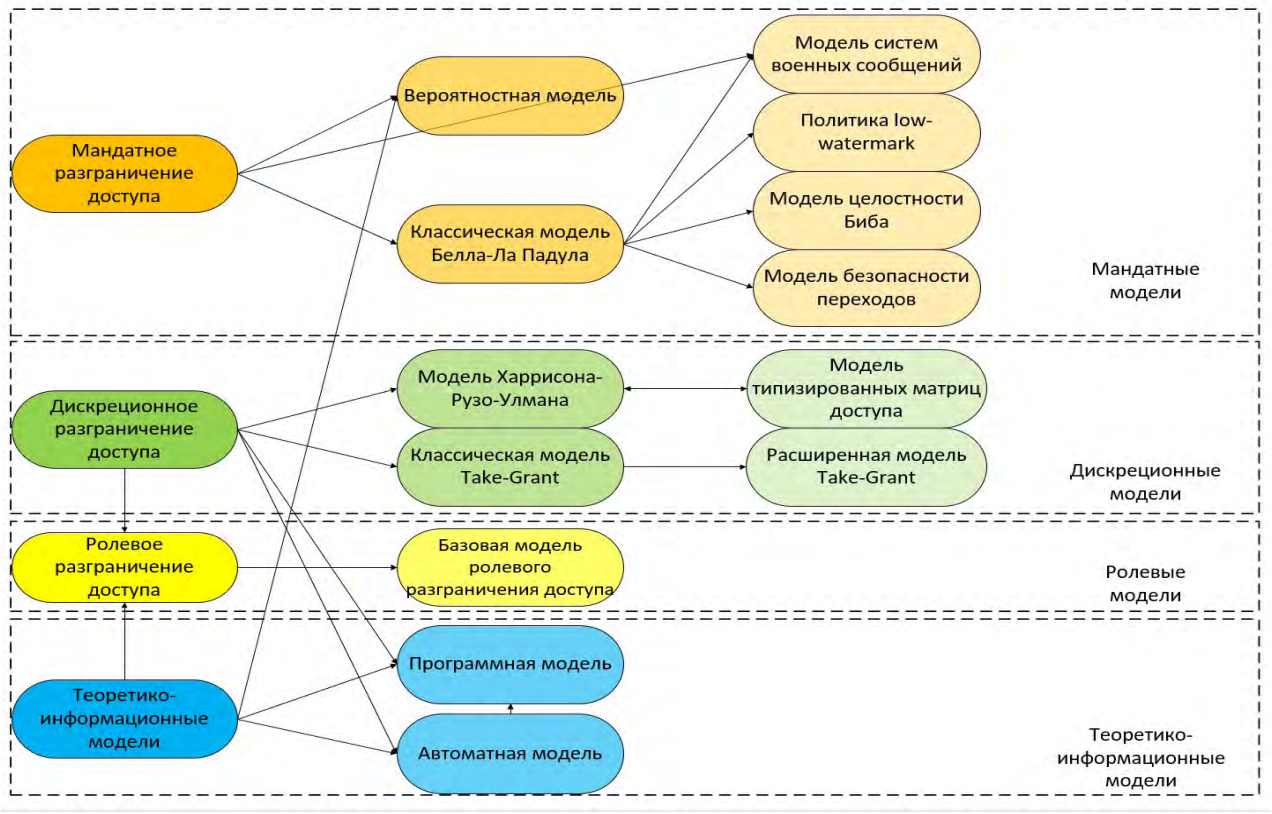

Рис. 4. Эволюция моделей управления доступом

управления доступом, в этой модели отсутствует учет атрибутов среды доступа и имеется ряд других ограничений, которые не позволяют в полной мере реализовать особенности закрытого документооборота в ЭОИС. В частности, изменение прав доступа не происходит до того момента, пока не будет осуществлено прерывание сеанса (перезагрузка системы). Данный факт определяет необходимость усовершенствования данной модели для реагирования на изменение прав доступа субъекта к объекту в режиме реального времени.

Среди подходов к усовершенствованию модели МРОСЛ-ДП наибольшего внимания, на наш взгляд, заслуживает ее дополнение решениями, заложенными в атрибутивной модели разграничения доступа – (Attribute-Based Access Control, ABAC) [16]. В модели ABAC разрешение на доступ к объектам выдается на основании проверки корректности выполнения множества правил, которые определяют используемую политику контроля доступа. При формировании правил используются три группы атрибутов: атрибуты пользователей (субъектов), атрибуты ресурсов (объектов) и атрибуты компьютерного окружения. К последней группе также относится время. По этой причине модель ABAC является достаточно гибкой и способной быстро реагировать на изменения.

Проблемным вопросом при использовании модели ABAC является верификация политик контроля доступа, так как в течение длительного времени работы с этой моделью возможно появление противоречивых правил доступа. Однако вполне возможно успешное решение этой проблемы на основе применения метода проверки на модели (model checking), в частности, как показали наши исследования, с использованием программного средства UPPAAL [17].

Подход к оптимизации схемы разграничения доступа

Ролевые возможности, присущие модели МРОСЛ-ДП, в условиях большой размерности системы управления доступа (большого количества пользователей и большого количества защищаемых ресурсов) приводят к необходимости решения NP-полной задачи извлечения ролей (Role Mining Problem, RMP) [18]. В этой задаче требуется найти оптимальную схему разграничения доступа, которая определяется отображениями вида «пользователи – роли» и «роли – права доступа», при заданном отображении вида «пользователи – права доступа». Оптимальность может рассматриваться по различным критериям, например, по минимальному количеству ролей в схеме доступа (ба-

зовая задача, Basic RMP) или по минимальному суммарному количеству связей в искомых отображениях (краевая задача, Edge RMP). В наших исследованиях показано, что в условиях большой размерности задачи RMP приемлемого времени ее решения возможно достичь при использовании усовершенствованного генетического алгоритма [19, 20].

К числу основных усовершенствований предлагаемого генетического алгоритма относятся:

- использование в качестве генов хромосом, которыми кодируются решения задачи RMP в генетическом алгоритме, не отдельных элементов булевых матриц, представляющих искомые отображения, а их столбцов, в результате чего значительно сокращается длина хромосом;
- каждая особь в популяции генетического алгоритма содержит не одну, как принято, а две независимые хромосомы, соответствующие двум искомым отображениям, в результате чего при выполнении операции скрещивания над родительскими особями получаются дочерние особи, находящиеся на достаточно большом расстоянии от родителей; это, в свою очередь, приводит к существенному снижению времени решения задачи;
- при скрещивании дочерних особей образуются не две, как в обычном алгоритме, а четыре особи-потомка ($2^2 = 4$), в результате чего увеличивается вероятность появления при скрещивании особей, соответствующих более предпочтительным решениям задачи;
- целевая функция (fitness-function) F генетического алгоритма формируется как взвешенная сумма двух вспомогательных функций, т.е. $F = w_1F_1 + w_2F_2$, где F_1 оценивает разницу между требуемой и текущей схемами доступа, а F_2 показывает количество ролей (для Basic RMP) или суммарное количество связей (для Edge RMP) в текущей схеме доступа. Управляя значениями весовых коэффициентов, можно управлять направлением поиска решения задачи. Например, можно настроить поиск таким образом, что вначале будет выполняться условие совпадения требуемой и текущей схемы доступа, а затем будет находиться минимальное количество ролей (связей);
- перед добавлением дочерних особей и особей, изменившихся во время выполнения операции мутации, в общую популяцию проводится проверка на их уникальность; тем самым предотвращается возможное «зацикливание» генетического алгоритма.

Проведенные эксперименты с предложенными усовершенствованными генетическими алгоритмами показали, что для больших размерностей задачи RMP, когда количество «пользователей» было несколько сотен или тысяч, количество итераций генетического алгоритма, требуемых для решения задачи, сокращалось на два – три порядка по сравнению с обычным генетическим алгоритмом. При этом наблюдалось линейное увеличение количества итераций при увеличении размерности задачи, что говорит о высокой масштабируемости предлагаемого подхода.

Подход к обнаружению попыток НСД на основе методов машинного обучения

Какой хорошей ни была бы модель управления доступом к ресурсам ЭИОС, все равно существует вероятность того, что достаточно квалифицированный пользователь-инсайдер будет предпринимать попытки НСД в обход правил доступа, установленных этой моделью. Поэтому представляется целесообразным реализация способов или подходов к защите от попыток НСД, не связанных с моделью управления доступом. Одним из таких подходов является обнаружение попыток НСД к базам данных ЭИОС, основанное на применении методов машинного обучения.

Проведенные нами исследования в этой области показали достаточно высокую эффективность такого подхода [21, 22, 23]. Его идея заключается в следующем. Наборы данных для обучения моделей машинного обучения (классификаторов) формируются из записей регистрационных журналов СУБД, в которых фиксируются все запросы, посланные на обработку пользователями. Множество признаков, определяющее структуру записей обучающих наборов данных, предлагается сформировать из следующих элементов: идентификаторов пользователей, количеств вхождений в запрос тех или иных ключевых слов языка запросов SQL и количеств вхождений в запрос имен таблиц данных и имен полей, к которым пользователи обращаются в своих запросах. Предполагается, что такого количества признаков будет вполне достаточно. В других известных исследований, посвященных применению методов машинного обучения для выявления аномальных SQL-запросов (например, в [24]) признаки выделяются на основании применения к SQL-запросам методов обработки текстов на естественном языке (Natural Language Processing, NLP). Однако методы NLP при достаточно больших разме-

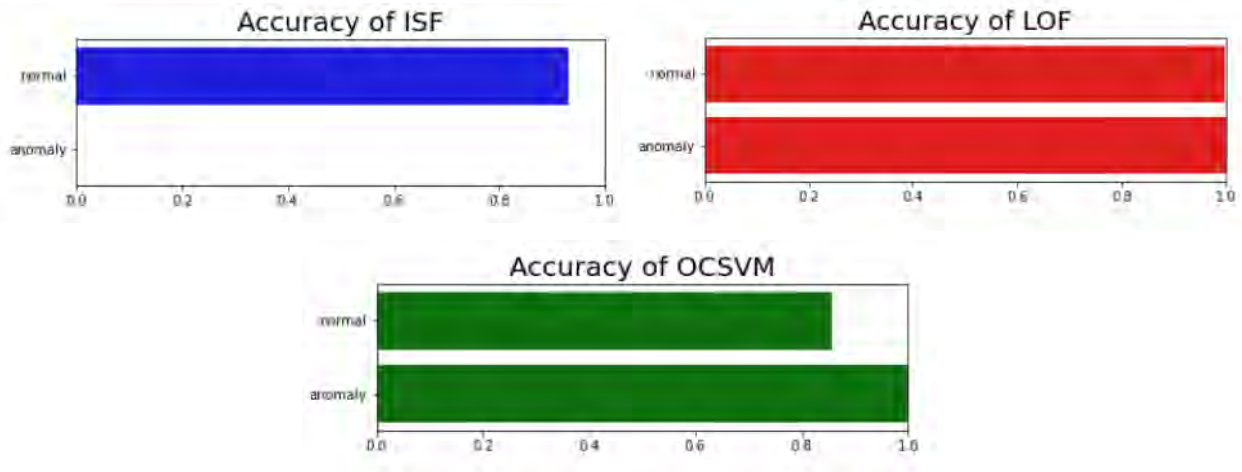

Рис. 5. Результаты, полученные при частично контролируемом обучении

рах обучающих наборов данных дают на порядок большее количество признаков. Это может привести не только к увеличению времени обучения и тестирования, но и к существенному снижению точности обнаружения аномальных запросов.

Для обнаружения аномальных запросов к базам данных ЭИОС, вызванных попытками НСД, исследовались модели неконтролируемого и частично контролируемого машинного обучения. Были выбраны следующие модели: метод *k*-средних (k-Means) совместно с методом главных компонент (Principal Component Analysis, PCA); изолированный лес (IF); локальный уровень выброса (LOF); одноклассный метод опорных векторов (OCSVM). Эксперименты проводились на наборах данных, полученных из регистрационных журналов СУБД PostgreSQL, работающей под Astra Linux, на которой была развернута база данных по планированию и ведению учебного процесса вуза. Всего обучающий набор данных, полученный из регистрационных журналов, содержал свыше 500 тысяч записей. Количество аномальных записей равнялось 20. Модели машинного обучения были реализованы в двух программных средах: на языке Python с наборами библиотек sklearn, numpy, pandas, matplotlib, Scipy, Re, Pylab и Math; в системе анализа данных с открытым исходным кодом Orange 3.32.

Исследование моделей неконтролируемого обучения показало, что все они дают большое количество ошибок первого и второго рода. Так, исследование модели k-Means показало, что ее наибольшая точность достигается при $k = 2$ и количестве кластеров, равном 5. Однако достигнутая точность была равна 0,82, что не в полной мере отвечает предъявляемым требованиям.

Иная картина получилась при исследовании моделей частично контролируемого обучения, когда обучение производится на наборе данных, содержащем только нормальные записи. Результаты, полученные на таком наборе данных для моделей IF, LOF и OCSVM, представлены на рисунке 5.

Точность обнаружения нормальных записей для модели LOF составила 0,9989, аномальных записей – 1,0. Модель ISF, не смотря на высокую точность обнаружения нормальных записей, не смогла обнаружить ни одной аномальной записи. Модель OCSVM показала точность обнаружения аномальных записей 1,0, однако для нормальных записей точность была равна всего лишь 0,8567.

На основании проведенных экспериментов сформирована таблица 1, в которой на основе сравнительной оценки отображаются предпочтения по использованию моделей машинного обучения для обнаружения SQL-запросов, содержащих попытки НСД.

Как видно из таблицы, наиболее предпочтительными являются модель LOF при неконтролируемом машинном обучении и модели LOF и OCSVM при частично контролируемом обучении. При этом модель LOF при частично контролируемом обучении обладает наибольшей предпочтительностью.

Заключение

Таким образом, в статье рассмотрены особенности функционирования ЭИОС вузов федеральных органов исполнительной власти и обоснована важность реализации системы управления доступом к

Таблица 1

Сравнительная оценка моделей машинного обучения

Вид машинного обучения	Модель машинного обучения	Оценка	Рекомендации
Неконтролируемое	K-Means	- -	-
	ISF	- -	-
	LOF	+ -	+
	OCSVM	- -	-
Частично контролируемое	ISF	- -	-
	LOF	+ +	+
	OCSVM	+ -	+

ресурсам ЭИОС. Рассмотрены три направления исследований, направленных на построение эффективной системы управления доступа, в которых авторами достигнуты определенные результаты. В направлении усовершенствования модели управления доступом предложен подход, предполагающий дополнение существующей модели решениями, имеющимися в модели ABAC. Для оптимизации схемы ролевого доступа предлагается использовать усовершенствованный генетический алгоритм. Для обнаружения попыток НСД к ресурсам ЭИОС предлагается использовать модели неконтролируемого и частично контролируемого машинного обучения, применяемые к наборам данных, сформированных из записей регистрационных журналов СУБД.

Дальнейшее направление исследований связывается с интеграцией результатов, полученных в предложенных подходах.

Рецензент: *Лаута Олег Сергеевич, доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, Санкт-Петербург, Россия. E-mail: laos-82@yandex.ru*

Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2022-0007.

Литература

1. Волков А.Г. Состояние и перспективы развития электронной информационно-образовательной среды в военной образовательной организации высшего образования // Гуманитарный вестник Военной академии Ракетных войск стратегического назначения. – 2017. – № 4 (8). – С. 14-21. eLIBRARY ID: 30793725.
2. Воронков И.Ю., Голубев М.А., Мержвинская Л.В., Репях Н.А. Методологические основы планирования деятельности военной образовательной организации в условиях внедрения электронной информационно-образовательной среды // Труды Военно-космической академии имени А.Ф. Можайского. – 2019. – № 671. – С. 393-400. eLIBRARY ID: 42680724.
3. Камыщенцев Ю.И. Образовательная и научная (научно-исследовательская) деятельность в формируемой электронной информационно-образовательной среде военного университета // Научно-методический бюллетень Военного университета МО РФ. – 2019. – № 12 (12). – С. 134-141. eLIBRARY ID: 43854579.
4. Рагозин А.Н. Перспективы и проблемы развития электронной информационно-образовательной среды высших военно-учебных заведений (на примере РВВДКУ) // Вестник военного образования. – 2021. – № 1 (28). – С. 22-26. eLIBRARY ID: 44664866.
5. Калиниченко И.А., Зиборов О.В., Ярмак К.В. Совершенствование электронной информационно-образовательной среды Московского университета МВД России имени В.Я. Кикотя // Вестник экономической безопасности. – 2019. – № 3. – С. 362-366. eLIBRARY ID: 41098316.
6. Локнов А.И. Развитие электронной информационно-образовательной среды в Санкт-Петербургском университете МВД России // Педагогика и психология в деятельности сотрудников правоохранительных органов: интеграция теории и практики. Материалы всероссийской научно-практической конференции. Под общей редакцией А.С. Душкина, Н.Ф. Гейжан. – 2019. – С. 229-233. eLIBRARY ID: 42370433.
7. Котенко П.К., Шевцов В.И. Электронная информационно-образовательная среда в системе государственной аккредитации образовательных организаций МЧС России // Перспективы науки и образования. – 2020. – № 1 (43). – С. 430-442. DOI: 10.32744/pse.2020.1.31
8. Булат Р.Е., Лебедев А.Ю., Никитин Н.А., Байчорова Х.С. Психолого-педагогические ресурсы повышения готовности обучающихся к образовательному процессу в условиях электронной информационно-образовательной среды // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – № 3. – С. 172-178. eLIBRARY ID: 44108918.

9. Воронов С.А., Рязанов Г.В. Электронная информационно-образовательная среда: опыт применения системы управления обучением Moodle в военной образовательной организации // Вестник Санкт-Петербургского военного института войск национальной гвардии. – 2021. – № 1 (14). – С. 11-15. eLIBRARY ID: 45617868.
10. Плюхин А.Ю. Электронная информационно-образовательная среда как средство формирования научно-исследовательской готовности преподавателей в вузах Росгвардии // Известия Воронежского государственного педагогического университета. – 2021. – № 4 (293). – С. 110-115.
11. Шкапенко Т.М. Электронное обучение: актуальное состояние проблемы в вузовской системе образования России и зарубежных стран // Вестник МГИМО Университета. – 2013. – № 6 (33). – С. 71-76. eLIBRARY ID: 20935584.
12. Калинин С.В., Левченко А.А., Федулов Б.А. Особенности реализации электронной информационно-образовательной среды юридического института МВД России при преподавании специальных дисциплин // Вестник Барнаульского юридического института МВД России. – 2019. – № 1 (36). – С. 183-185. eLIBRARY ID: 38510928.
13. Митрошин П.А. Разработка отказоустойчивой электронной информационно-образовательной среды учебного заведения с учётом требований информационной безопасности // Технологии техносферной безопасности. – 2021. – № 3 (93). – С. 73-87. DOI: 10.25257/TTS.2021.3.93.73-87.
14. ГОСТ Р 59383-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. Дата введения 2021-11-30 / Федеральное агентство по техническому регулированию. – М.: Стандартинформ, 2021.
15. Девянин П.Н., Кулямин В.В., Петренко А.К., Хорошилов А.В., Щепетков И.В. Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы // Труды Института системного программирования РАН. – 2020. – Т. 32, № 1. – С. 7-26. DOI: 10.15514/ISPRAS-2020-32(1)-1.
16. Hu V.C., Kuhn R., Ferraiolo D., Voas J. Attribute-based access control // Computer. – 2015. – Vol. 48, No. 2. – Pp. 85-88. DOI: 10.1109/MC.2015.33.
17. Котенко И. В., Левшун Д. С., Саенко И. Б. Верификация политик разграничения доступа на основе атрибутов в облачных инфраструктурах с помощью метода проверки на модели // Системы управления, связи и безопасности. – 2019. – № 4. – С. 421-436. DOI: 10.24411/2410-9916-2019-10417.
18. Саенко И.Б., Бирюков М.А., Ясинский С.А., Грязев А.Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. – 2018. – № 1. – С. 81-85. eLIBRARY ID: 34859229.
19. Saenko I., Kotenko I. Design and performance evaluation of improved genetic algorithm for Role Mining Problem // Proceedings of the 2012 20th Euromicro International Conference on Parallel, Distributed and Network-based Processing, Munich, Germany, 2012. – pp. 269-274. DOI: 10.1109/PDP.2012.31.
20. Kotenko I., Saenko I. Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks // International Journal of Bio-Inspired Computation. – 2015. – Vol. 7, No. 2. – pp. 98-110. DOI: 10.1504/IJBIC.2015.069291.
21. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. – 2022. – № 2 (48). – С. 87-97. DOI: 10.21681/2311-3456-2022-2-87-97.
22. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Исследование возможностей выявления аномального поведения пользователей центров обработки данных на моделях машинного обучения // Двадцатая Национальная конференция по искусственному интеллекту с международным участием, КИИ-2022 (Москва, 21–23 декабря 2022 г.). Труды конференции. В 2 т. Т. 2. – М.: Издательство МЭИ, 2022. – С. 232-241. eLIBRARY ID: 50178696.
23. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. – 2018. – Vol.6. – pp. 72714-72723. DOI: 10.1109/ACCESS.2018.2881998.
24. Gowtham M., Pramod H.B. Semantic Query-Featured Ensemble Learning Model for SQL-Injection Attack Detection in IoT-Ecosystems // IEEE Transactions on Reliability. – 2022. – Vol. 71, No. 2. – pp. 1057-1074. DOI: 10.1109/TR.2021.3124331.

MANAGEMENT OF ACCESS TO ELECTRONIC INFORMATION AND EDUCATIONAL ENVIRONMENT OF UNIVERSITIES OF FEDERAL EXECUTIVE AUTHORITIES

Kotenko I.V. [6], Saenko I.B.[7], Zakharchenko R.I,[8], Kapustin A.S.[9], Mazen Al-Barri[10]

6 Igor V. Kotenko, Doctor of Technical Sciences, Professor, Chief Scientist and Head of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

7 Igor B. Saenko, Doctor of Technical Sciences, Professor, Leading researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ibsaen@comsec.spb.ru

8 Roman I. Zakharchenko, Doctor of Technical Sciences, Head of the Department at Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: romanzakharchenko@yandex.ru

9 Alexander S. Kapustin, Adjunct at Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: redbull1666@mail.com

10 Mazen Kh. Al-Barri, Adjunct at Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail: mazenb51@gmail.com

The purpose of the article: *analysis of the problem of ensuring timely authorized access to the resources of the electronic information and educational environment of universities of federal executive authorities and identification of possible directions for its solution.*

Research methods: *system analysis of the problem of ensuring access of officials of universities of federal executive authorities to the resources of the electronic information and educational environment.*

The result obtained: *approaches to improving the existing access control model, optimizing the role-based access scheme and determining unauthorized access attempts based on machine learning methods are proposed.*

Scope of the proposed approach: *access control system of the electronic information and educational environment of universities of federal executive authorities.*

Scientific novelty: *consists in a comprehensive analysis of the problem of creating and functioning of the electronic information and educational environment of universities of federal executive authorities, during which the structure of this environment is determined and its characteristic features are highlighted. Based on the analysis of information security threats in the electronic information and educational environment, the necessity of creating an access control system to its resources, which provides timely authorized access, is substantiated. The proposed approaches to improving the access control system affect not only the improvement of the existing access model by supplementing it with solutions available in the attribute-based access model, but also the optimization of the role-based access scheme using the developed genetic algorithm and the detection of unauthorized access attempts associated with overcoming access rules, based on application of machine learning methods. Experimental results are presented that confirm the effectiveness of the proposed approaches.*

Contribution: *Igor Kotenko – analysis of the state of the art in the creation and application of the electronic information and educational environment of universities of federal executive authorities, setting the task and developing proposals for developing the functionality of the access control system, development of approaches to genetic optimization of the access scheme and detection of unauthorized access attempts using machine learning methods; Igor Saenko – development of approaches to improving the access control system related to the use of an attribute-based access model, genetic optimization of the access scheme and detection of unauthorized access attempts using machine learning methods; Roman Zakharchenko – analysis of technical solutions that ensure the implementation of the access control system to the resources of the electronic information and educational environment of universities of federal executive authorities, Alexander Kapustin – analysis of security threats and access control models to resources of the electronic information and educational environment of universities of federal executive authorities, Mazen Al-Barri – development and experimental study of an approach to detect attempts of unauthorized access to the resources of the electronic information and educational environment of universities of federal executive authorities, based on the use of machine learning methods.*

Keywords: *cybersecurity, electronic information and educational environment, access control model, mandatory access control, role-based access control, genetic algorithm, machine learning.*

References

1. Volkov A.G. Status and development prospects of the electronic information and educational environment in the military educational organization of higher education // Humanitarian Bulletin of the Military Academy of Strategic Missile Forces. – 2017. – No. 4 (8). – pp. 14-21. (in Russian)
2. Voronkov I.Yu., Golubev M.A., Merzhvinskaya L.V., Repyakh N.A. Methodological bases for planning the activities of a military educational organization in the context of the introduction of an electronic information and educational environment // Proceedings of the Military Space Academy named after A.F. Mozhaisky. – 2019. – No. 671. – pp. 393-400. (in Russian)
3. Kamyshentsev Yu.I. Educational and scientific (research) activity in the formed electronic information and educational environment of the military university // Scientific and methodological bulletin of the Military University of the Ministry of Defense of the Russian Federation. – 2019. – No. 12 (12). – pp. 134-141. (in Russian)
4. Ragozin A.N. Prospects and problems of development of the electronic information and educational environment of higher military educational institutions (on the example of the RVVDKU) // Bulletin of military education. – 2021. – No. 1 (28). – pp. 22-26. (in Russian)
5. Kalinichenko I.A., Ziborov O.V., Yarmak K.V. Improving the electronic information and educational environment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot // Bulletin of economic security. – 2019. – No. 3. – pp. 362-366. (in Russian)
6. Loknov A.I. Development of an electronic information and educational environment at the St. Petersburg University of the Ministry of Internal Affairs of Russia // Pedagogy and psychology in the activities of law enforcement officers: integration of theory and practice.

Materials of the All-Russian scientific-practical conference. A.S. Dushkina, N.F. Geizhan (Eds.). – 2019. – pp. 229-233. (in Russian)
7. Kotenko P.K., Shevtsov V.I. Electronic Information and Educational Environment in the System of State Accreditation of Educational Organizations of the Ministry of Emergency Situations of Russia // Prospects of Science and Education. – 2020. – No. 1 (43). – pp. 430-442. DOI: 10.32744/pse.2020.1.31. (in Russian)
8. Bulat R.E., Lebedev A.Yu., Nikitin N.A., Baichorova Kh.S. Psychological and pedagogical resources for increasing the readiness of students for the educational process in the conditions of an electronic information and educational environment // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". – 2020. – No. 3. – pp. 172-178. (in Russian)
9. Voronov S.A., Ryazanov G.V. Electronic information and educational environment: the experience of using the Moodle learning management system in a military educational organization // Bulletin of the St. Petersburg Military Institute of the National Guard Troops. – 2021. – No. 1 (14). – pp. 11-15. (in Russian)
10. Plyukhin A.Yu. Electronic Information and Educational Environment as a Means of Forming the Research Readiness of Teachers in the Higher Educational Institutions of the National Guard // Bulletin of the Voronezh State Pedagogical University. – 2021. – No. 4 (293). – pp. 110-115. (in Russian)
11. Shkapenko T.M. E-learning: the current state of the problem in the higher education system in Russia and foreign countries // Bulletin of MGIMO University. – 2013. – No. 6 (33). – pp. 71-76. (in Russian).
12. Kalinin S.V., Levchenko A.A., Fedulov B.A. Features of the implementation of the electronic information and educational environment of the legal institute of the Ministry of Internal Affairs of Russia in the teaching of special disciplines // Bulletin of the Barnaul Law Institute of the Ministry of Internal Affairs of Russia. – 2019. – No. 1 (36). – pp. 183-185. (in Russian).
13. Mitroshin P.A. Development of a fault-tolerant electronic information and educational environment of an educational institution, taking into account the requirements of information security // Technology of technosphere safety. – 2021. – No. 3 (93). – pp. 73-87. DOI: 10.25257/TTS.2021.3.93.73-87. (in Russian)
14. GOST R 59383-2021. Information Technology. Methods and means of ensuring security. Access control basics. Introduction date 2021-11-30 / Federal Agency for Technical Regulation. – M.: Standartinform, 2021. (in Russian)
15. Devyanin P.N., Kulyamin V.V., Petrenko A.K., Khoroshilov A.V., Shchepetkov I.V. Integration of mandatory and role-based access control and mandatory integrity control in a verified hierarchical security model of an operating system // Proceedings of ISP RAS. – 2020. – Vol. 32, No. 1. – pp. 7-26. DOI: 10.15514/ISPRAS-2020-32(1)-1. (in Russian)
16. Hu V.C., Kuhn R., Ferraiolo D., Voas J. Attribute-based access control // Computer. – 2015. – Vol. 48, No. 2. – pp. 85-88. DOI: 10.1109/MC.2015.33.
17. Kotenko I. V., Levshun D. S., Saenko I. B. Verification of Attribute-Based Access Control Policies in Cloud Infrastructures Using the Model Check Method // Control Systems, Communications and Security. – 2019. – No. 4. – pp. 421-436. DOI: 10.24411/2410-9916-2019-10417. (in Russian)
18. Saenko I.B., Biryukov M.A., Yasinsky S.A., Gryazev A.N. Implementation of security criteria when building a unified system for restricting access to information resources in cloud infrastructures // Information and space. – 2018. – No. 1. – pp. 81-85. (in Russian).
19. Saenko I., Kotenko I. Design and performance evaluation of improved genetic algorithm for Role Mining Problem // Proceedings of the 2012 20th Euromicro International Conference on Parallel, Distributed and Network-based Processing, Munich, Germany, 2012. – pp. 269-274. DOI: 10.1109/PDP.2012.31.
20. Kotenko I., Saenko I. Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks // International Journal of Bio-Inspired Computation. – 2015. – Vol. 7, No. 2. – pp. 98-110. DOI: 10.1504/IJBIC.2015.069291.
21. Saenko I.B., Kotenko I.V., Al-Barri M.H. The use of artificial neural networks to detect anomalous behavior of users of data processing centers // Voprosy kiberbezopasnosti. – 2022. – No. 2 (48). – pp. 87-97. DOI: 10.21681/2311-3456-2022-2-87-97. (in Russian)
22. Saenko I.B., Kotenko I.V., Al-Barri M.H. Research on the possibilities of detecting anomalous behavior of data center users using machine learning models // Twentieth National Conference on Artificial Intelligence with International Participation, KII-2022 (Moscow, December 21–23, 2022). Proceedings of the conference. Vol. 2. – M.: MPEI Publishing House, 2022. – pp. 232-241. (in Russian).
23. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. – 2018. – Vol.6. – pp. 72714-72723. DOI: 10.1109/ACCESS.2018.2881998.
24. Gowtham M., Pramod H.B. Semantic Query-Featured Ensemble Learning Model for SQL-Injection Attack Detection in IoT-Ecosystems // IEEE Transactions on Reliability. – 2022. – Vol. 71, No. 2. – pp. 1057-1074. DOI: 10.1109/TR.2021.3124331.