ПРОЕКТИРОВАНИЕ МЕХАНИЗМОВ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА И АУДИТА БЕЗОПАСНОСТИ В ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Зиннатуллина А.А., ассистент,
Сайфуллина Ю.И., студент,
Хайбуллина А.А., студент,
БашГАУ, г. Уфа, Россия

Аннотация. Статья посвящена проектированию связки из ролевой модели доступа и журнала аудита для прикладной системы. Рассмотрены модели RBAC и ABAC, требования ФСТЭК России и данные OWASP по нарушениям контроля доступа. Расчётная модель для 500 пользователей показала снижение числа записей о правах с 25 000 до 860.

Ключевые слова: разграничение доступа, RBAC, ABAC, аудит безопасности, журнал событий, ФСТЭК, OWASP, прикладная информационная система

Права доступа ломаются раньше, чем шифрование.В редакции OWASPTop 10 за 2021 год нарушение контроля доступа поднялось с пятого места на первое, а тестами на него было охвачено до 94,55% приложений выборки [5]. Для прикладной системы это означает простую вещь. Сотрудник открывает чужую карточку клиента, меняет число в адресной строке и получает данные, к которым доступа не имел.

Цель статьи состоит в проектировании схемы ролевого доступа и журнала аудита, которые можно реализовать в учебной конфигурации 1С или в веб-приложении на PHP. Были поставлены три задачи. Сравнить модели RBAC и ABAC, сопоставить схему с требованиями ФСТЭК России и посчитать, насколько

роли сокращают объём администрирования. Данных о внедрении в конкретной организации нет, поэтому часть выводов опирается на расчёт, а не на замеры.

Идея ролей старше веба. Феррайоло и соавторы предложили в 2001 году для NIST стандарт из четырёх компонентов. Это базовая модель, иерархия ролей, статическое и динамическое разделение обязанностей [3]. Права в ней привязываются к должности, а не к человеку.

Модель ABAC описана в NISTSP 800-162 в 2014 году. Решение там зависит от атрибутов субъекта, объекта и среды, например от времени суток или подразделения [4]. Прямого сравнения стоимости внедрения RBAC и ABAC в использованных источниках нет, поэтому выбор сделан по масштабу задачи.

Для учебной системы на 100-500 пользователей выбрана ролевая модель с одним атрибутным условием. Например, кладовщик видит остатки только своего склада. В 1С эта связка уже знакома по профилям групп доступа и ограничениям на уровне записей. Полностью атрибутная схема на таком масштабе добавила бы сложность без заметной пользы, и это личная оценка авторов.

Закон требует защиты от неправомерного доступа.Федеральный закон № 152-ФЗ от 27.07.2006 обязывает оператора защищать персональные данные от неправомерного доступа [1]. Конкретные меры для государственных информационных систем задаёт ФСТЭК России. С 1 марта 2026 года приказ № 17 от 11.02.2013 заменён приказом № 117 от 11.04.2025 [2].

Перечень мер нового приказа в рамках статьи полностью не сверялся, поэтому соответствие каждой мере не заявляется. Роли, сроки бездействия сеанса и журнал входов заложены в проект как минимальный набор.

Схема данных укладывается в шесть таблиц.Пользователи, роли, права, связь пользователь-роль, связь роль-право и журнал событий. Проверка идёт на сервере при каждом запросе, а по умолчанию действует запрет, как рекомендует OWASP для всего, кроме публичных ресурсов [5]. Статическое разделение

обязанностей из стандарта NIST запрещает одному человеку одновременно создавать и утверждать платёж [3].

Журнал фиксирует пять полей. Кто выполнил действие, что именно, над каким объектом, когда и с какого адреса, а также результат. Записываются входы и неудачные попытки, смена ролей, выгрузки и удаления. Для учебной базы заложено хранение журнала в отдельной таблице без права изменения у прикладных ролей.

Данных о реальном объёме журнала нет. Оценка в 20-50 записей на пользователя в день взята как рабочее допущение и в расчётах не используется.

Первый результат относится к рискам.В данных OWASP на 34 типа слабостей приходится 318 487 случаев и 19 013 уязвимостей из базы CVE, а средняя доля приложений с хотя бы одной такой слабостью равна 3,81% при максимуме 55,97% [5]. Разрыв между средним и максимальным значением виден на рис. 1. У отдельных команд проблема носит системный характер.

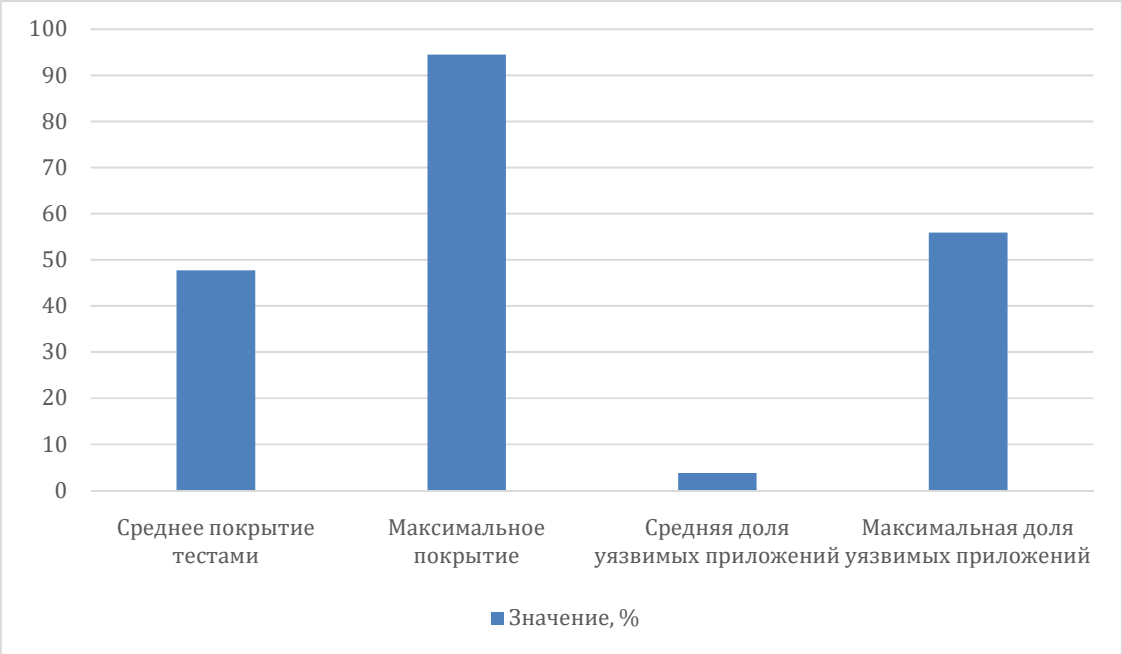

Рис. 1. Покрытие тестами и доля уязвимых приложений по категории нарушения контроля доступа, OWASP, 2021



Рис. 2. Число записей о назначении прав при прямой выдаче и ролевой модели

Второй результат получен расчётом. Принято 8 ролей по 45 прав и 50 прав на пользователя при прямой выдаче. Для 50 пользователей получается 2 500 записей против 410, для 150 пользователей 7 500 против 510, для 500 пользователей 25 000 против 860. Выигрыш растёт с 6,1 до 29,1 раза (рис. 2). Допущения условные, реальные цифры зависят от числа должностей.

На практике это выглядит так. Когда бухгалтеру добавляют право на закрытие периода, при прямой выдаче правят 20 учётных записей, при ролевой одну.

Расчёт не заменяет замеры.Модель предполагает, что роли заданы без пересечений. На практике сотрудники совмещают должности, и число ролей растёт быстрее, чем в расчёте, так что реальный выигрыш будет меньше 29,1 раза. Эмпирической проверки в живой организации не проводилось. Кроме того, данные OWASP описывают веб-приложения разных команд, а не учебные конфигурации 1С, и переносить их напрямую нельзя.

В итоге схема из ролей, одного атрибутного условия и неизменяемого журнала закрывает базовые требования и остаётся проверяемой. Какую долю инцидентов она предотвратит, по имеющимся данным оценить нельзя.

Литература

1. О персональных данных :федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ : принят Гос. Думой 8 июля 2006 г. : одобр. Советом Федерации 14 июля 2006 г. // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1). Ст. 3451.

2. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : приказ ФСТЭК России от 11 апр. 2025 г. № 117 // Официальный интернет-портал правовой информации. URL: pravo.gov.ru (дата обращения: 13.11.2026). (Примечание: если вы брали документ из КонсультантПлюс или Гаранта, замените источник опубликования на соответствующую СПС).

3. Proposed NIST standard for role-based access control / D. F. Ferraiolo [et al.] // ACM Transactions on Information and System Security. 2001. Vol. 4, № 3. P. 224–274.

4. Guide to attribute based access control (ABAC) definition and considerations : NIST Special Publication 800-162 / V. C. Hu [et al.]. Gaithersburg : NIST, 2014. 54 p.

5. A01:2021 – Broken Access Control // OWASP Top 10:2021. URL: owasp.org (датаобращения: 13.11.2026).