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.

...

полный текст во вложении