DOI: 10.18372/2410-7840.23.16406
УДК 004.658.2

КЕРУВАННЯ ДОСТУПОМ НА ОСНОВІ АТРИБУТІВ В ІНФОРМАЦІЙНИЙ СИСТЕМАХ КЛАСУ CRM ТА ERP

Лях Дар'я, Коломицев Михайло, Носок Світлана

Ефективне керування процесами в компанії в наші дні не може обійтись без автоматизації. Використання CRM та ERP систем сприяє підвищенню ефективності, автоматизації та оптимізації більшості процесів на підприємстві. Впроваджуючи CRM або ERP систему кожна компанія обов'язково замислюється про забезпечення безпеки своїх даних, а отже і забезпечення чіткого та надійного керування доступом до всіх даних в системі. В роботі було проаналізовано дві найбільш поширені на сьогодні політики керування доступом – рольову політику керування доступом (RBAC) та політику керування доступом на основі атрибутів (ABAC). Керування доступом на основі атрибутів називають майбутнім керування доступом через забезпечення впровадження складних політик та залежності рішення про дозвіл або заборону доступу не тільки від ролі користувача, а також і інших параметрів суб'єкту, об'єкту та середовища, вона надає значно більше можливостей впровадження гнучких політик керування доступом. Також було досліджено наявні політики керування доступом ERP системи – Microsoft Dynamics AX та CRM системи - Microsoft Dynamics CRM, їх специфічні особливості. Сформовано ряд вимог які не покриває поточна реалізація керування доступом в цих системах, проте може задовольнити політика керування доступом на основі атрибутів. В роботі було розроблено власну систему атрибутів, специфічну для даних систем, яку можна використати для реалізації рішення щодо впровадження політики керування доступом на основі атрибутів до CRM та ERP систем Microsoft Dynamics 365. Було також розроблено універсальне рішення для впровадження політики керування доступом на основі атрибутів для системи Microsoft Dynamics CRM, яке може бути використане, як в якості заміни існуючої рольової системи керування доступом, так і разом з нею для підвищення ефективності системи керування доступом.

Ключові слова: *керування доступом на основі атрибутів (ABAC), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP).*

ВСТУП

Коли компанії проходять цифрову трансформацію, вони, як правило, намагаються підвищити ефективність у критичних бізнес-процесах, а також високий рівень наочності цих процесів.

З усіх цих процесів є багато таких, які є фундаментальною основою того, як працює підприємство. Тому дуже важливо мати більший контроль над цими робочими процесами, ніж минулі роки.

Інвестування в такі технології, як програмне забезпечення для планування ресурсів підприємства (ERP) та програмне забезпечення управління відносинами з клієнтами (CRM), допомагає підвищити ефективність у критичних бізнес-процесах, а також високий рівень наочності цих процесів.[1]

Системи ERP і CRM наповнені конфіденційними даними та інформацією. Вони містять дані про фінанси організації, її співробітників, процеси, клієнтів та багато іншого.

Якщо ці дані не будуть належним чином захищені, це може призвести до значних наслідків: втрата грошей та завдання шкоди репутації компанії.

Метою роботи є дослідження системи керування доступом інформаційних систем класу CRM та ERP та покращення існуючої системи за допомогою впровадження керування доступом на основі атрибутів.

Актуальність даної роботи випливає з росту популярності використання CRM та ERP систем. Ключовим аспектом безпеки, відповідальність за реалізацію якого лежить не на боці постачальника, а на боці клієнта є політика керування доступом.

Для багатьох клієнтів є важливою можливість реалізації більш гнучких та динамічних налашту-

вань, які не може задовольнити існуюча система керування доступом.

ПОЛІТИКИ КЕРУВАННЯ ДОСТУПОМ

Політика керування доступом – це сукупність функцій, які визначають, чи запрошена операція над спільним об'єктом є законною чи ні.

Політики контролю доступу використовують правила розмежування доступу, щоб визначити, який користувач може отримати які типи доступу до спільного ресурсу. Вони керують всіма правами доступу та конфліктами доступу щодо спільних ресурсів.

Вже було розроблено досить багато моделей контролю доступу і кожна з них має свої переваги в деяких ситуаціях.

Ключовими механізмами є дискретний (DAC – Discretionary Access Control), мандатний (MAC – Mandatory Access Control), такий, що використовує ролі (RBAC – Role-based access control) та такий, що використовує атрибути (ABAC – Attribute-based access control).

У методі керування доступом, що використовує ролі (RBAC), права доступу також визначає система. Ролі відповідає множина прав доступу до ресурсів. Механізм RBAC дає змогу визначати доступ до складних бізнес-операцій, наприклад, транзакцій.

Користувачі отримують відповідні права через зв'язок з певними ролями. Ролі об'єднуються в ієрархії, у яких дозволи ролей вищих рівнів успадковуються на нижчих рівнях.

Керування доступом з використанням ролей має найбільший ефект, коли на підприємстві є багато користувачів з однаковими наборами прав доступу, які і зводяться до визначених ролей.

Зміна прав доступу для ролі відразу діє для усіх асоційованих з цією роллю користувачів. Керування доступом на базі ролей сьогодні є одним з найкращих підходів до керування доступом. У RBAC права доступу призначаються адміністратором вручну та є статичними.

Оскільки RBAC використовує статичні асоціації, він не може задовольнити потреби безпеки систем, що вимагають динамічних асоціацій та незалежних від ролі політик безпеки.[2] ABAC вирішує цю проблему і здатний виконувати динамічні відносини та генерувати незалежні від ролей політики безпеки, використовуючи колекції атрибутів, згрупованих у чотири категорії:

- Атрибути про суб'єкт, тобто користувач, який робить запит. Це може включати його ім'я користувача, будь-які групи, до яких вони належать, спосіб автентифікації тощо.
- Атрибути про ресурс або об'єкт, до якого здійснюється доступ, наприклад, URI ресурсу або мітка безпеки.
- Атрибути дії, яку намагається виконати користувач, наприклад оновити запис.
- Атрибути про середовище або контекст, у якому відбувається операція. Це може включати місцевий час доби або місцезнаходження користувача, який виконує дію [3].

І RBAC, і ABAC відповідають потребам безпеки великих програм або організацій, але ABAC відповідає складним вимогам безпеки сучасних систем. Він забезпечує кращу безпеку, навіть якщо зв'язок між суб'єктами та об'єктами зростає в геометричній прогресії.

РЕАЛІЗАЦІЯ КЕРУВАННЯ ДОСТУПОМ У ІНФОРМАЦІЙНИХ СИСТЕМАХ КЛАСУ CRM ТА ERP.

Системи CRM допомагають керувати даними клієнтів, покупками та контактною інформацією, аналізувати та розуміти їх для збільшення продажів. Підприємства використовують CRM для кращого розуміння своїх клієнтів, для прийняття більш обґрунтованих рішень щодо продажу та взаємодії з ними.

Системи ERP використовуються для управління бізнесом. Як і CRM, ERP дозволяє швидко обмінюватися стандартизованою інформацією між всіма відділами.

Усі співробітники вводять інформацію до системи ERP, створюючи в реальному часі загальний знімок всього підприємства. Дозволяючи бізнесу зосереджуватися на даних, а не на операціях, ERP надає метод для спрощення бізнес-процесів.

1. Microsoft Dynamics CRM

Система керування доступом Microsoft Dynamics CRM також заснована на рольовій мо-

делі. Для контролю доступу до даних необхідно створити організаційну структуру, яка захищає конфіденційні дані і забезпечує спільну роботу, а саме налаштувати бізнес-підрозділи, ролі безпеки і профілі безпеки поля. Ролі безпеки визначають, які дії користувач може виконати над записом.

Крім того, є кілька підходів до безпеки. Наприклад, доступ до кожного запису зазвичай базується на моделі власності. Наприклад, я можу читати лише свої облікові записи. Але існують інші варіанти, такі як ієрархічна безпека.[4]

Ключові аспекти, на яких базується безпека в Microsoft Dynamics CRM:

- Команди – об'єднують користувачів та зв'язані з ролями безпеки.
- Ролі безпеки – дозволяють визначити, який доступ буде наданий командам та користувачам. Спочатку створюються ролі, а потім одна або кілька асоціюються з кожним користувачем/командою.
- Бізнес-одиниці (business units) – фундаментальний будівельний блок у моделі безпеки Dynamics. Вони визначають структуру організації.
- Профілі безпеки поля (field security profile) – використовуються, коли потрібно визначити конкретні права доступу до окремих полів (можна дозволити або заборонити ролі доступ на читання, створення або оновлення інформації у деякому полі).
- Ієрархічна безпека: підтримує модель безпеки на основі ієрархії організаційної структури підприємства.

2. Microsoft Dynamics AX

Microsoft Dynamics AX (Axapta) – це багатофункціональна ERP-система для управління ресурсами підприємства для середніх та великих компаній з розподіленою структурою. Вона охоплює всі області менеджменту: виробництво та дистрибуцію, ланцюжки поставок і проекти, фінанси та засоби бізнес-аналізу, взаємовідносини з клієнтами та персоналом.[5] Її остання версія – Dynamics 365 for Finance and Operations. У Dynamics 365 for Finance and Operations можна використовувати привілеї для групування захищених об'єктів, таких як точки входу та дозволи для таблиць, форм і звітів. Крім того, можна об'єднати привілеї в обов'язки і обов'язки в цикли процесу. Обов'язок – це набір привілеїв доступу до програм, необхідних користувачеві для виконання своїх обов'язків. Процесний цикл – це сукупність обов'язків, які представляють бізнес-процес більш високого рівня. Модель безпеки є ієрархічною, і кожен елемент в ієрархії представляє різний рівень деталізації.[6]

Система керування доступом Microsoft Dynamics AX заснована на рольовій моделі. Доступ до системи дозволений лише авторизованим користувачам, кожен з яких повинен мати певні ролі. Ролям призначається певний набір привілеїв доступу до програми. Користувачі можуть бути призначені для однієї або кількох ролей безпеки і за допомогою цих призначень ролей отримати дозволи на виконання певних системних функцій. Користувач, якому призначено роль безпеки, має доступ до набору привілеїв, пов'язаних з цією роллю. Усім користувачам потрібно призначити принаймні одну роль безпеки, щоб мати доступ до системи. Ролі безпеки, які призначаються користувачеві, визначають обов'язки, які він може виконувати, і частини інтерфейсу користувача, які користувач може переглядати.[6]

ПЕРЕВАГИ ABAC НАД RBAC ДЛЯ CRM ТА ERP

Рольовий контроль доступу був розроблений для більш простого світу. Формалізований NIST у 1992 році, RBAC швидко став стандартом для підприємств, які керують понад 500 співробітниками. Перевершуючи попередні моделі, RBAC був значною мірою реалізований у системах забезпечення користувачів, що дало підприємствам можливість керувати контролем доступу за ролями, а не індивідуальним ідентифікатором користувача працівника.[7] Впровадження контролю доступу на основі атрибутів, дозволяє безпечно ділитися конфіденційною інформацією та дотримуватись вимог нормативних даних. ABAC дозволяє створювати елементи керування на основі характеристик даних.

Додаючи контекст, рішення про надання доступу можна приймати не лише на основі ролі користувача, але й з урахуванням того, з ким він має відношення, до чого потрібен доступ цього

користувача, звідки йому потрібен доступ, коли цей доступ потрібен. ABAC робить це, використовуючи політики, побудовані на індивідуальних атрибутах.

Створюючи політику, яку легко зрозуміти, з контекстом навколо користувача та до того, до чого він має мати доступ, контроль доступу стає набагато більш надійним.

В CRM та ERP системах використовується рольова політика керування доступом. Проте є чимало вимог, які можуть бути важливими та навіть критичними для підприємств, що використовують CRM та ERP системи, для реалізації яких наявних систем контролю доступу недостатньою, проте при впровадженні системи доступу заснованої на атрибутах, їх можна задовольнити:

- Обмеження часу доступу до ресурсів: наявні політики не дозволяють обмежити час доступу до певних ресурсів для окремих користувачів, тільки для всієї системи в цілому.

- Доступ на виконання операції над об'єктом повинен залежати від інформації про об'єкт: В системах немає можливості впроваджувати складні правила доступу. Наприклад, рядовий співробітник не має права завершувати продаж, якщо сума продажу перевищує ліміт.

- Доступ на виконання операції над об'єктом повинен залежати від інформації про суб'єкт: в системах немає можливості впроваджувати складні правила доступу. Наприклад, рядовий співробітник не має права завершувати продаж, якщо число затверджень перевищує ліміт затверджень користувача.

- Обмеження доступу до нового функціоналу: при впровадженні CRM та ERP систем в більшості компанії не користуються тільки стандартним функціоналом системи, а також впроваджують власні додаткові процеси, які можуть, наприклад, змінювати якісь дані чи інтегруватися з зовнішньою системою. Існуючою рольовою політикою не має можливості керувати доступом до цих процесів.

- Права повинні динамічно змінюватися при зміні посади співробітника: Наразі ролі можуть бути назначені тільки відповідальним співробітником, а не змінені автоматично.

- Обмежити права доступу системного адміністратора: за замовчуванням роль системного адміністратора не можна модифікувати, проте іноді цю роль необхідно надати користувачу наприклад для впровадження кастомізацій до системи. В такому випадку користувач буде мати доступ до ресурсів та чуттєвих даних.

Для можливості більш гнучких налаштувань безпеки необхідна реалізація системи доступу на основі атрибутів. Оскільки, перш за все, не можливо вимкнути існуючу рольову політику керування доступом, найкращим рішенням буде скомбінувати обидві моделі – наявну рольову та модель, на основі атрибутів. Поєднання RBAC і ABAC може допомогти адміністраторам отримати найкраще з обох систем. RBAC і ABAC можна використовувати разом ієрархічно, з широким доступом, забезпеченим протоколами RBAC, і більш складним доступом, керованим ABAC. Їх змішування поєднує в собі сильні сторони обох.

РОЗРОБКА СИСТЕМИ АТРИБУТІВ ДЛЯ CRM ТА ERP

Проаналізувавши можливості системи безпеки Microsoft Dynamics CRM та Microsoft Dynamics AX було розроблено власну систему атрибутів для керування доступом для виконання деяких дій в системі:

Суб'єкт, що здійснює ді:
- безпосередньо користувач;
- посада користувача;
- бізнес-одиниця користувача;
- ролі користувача;
- команда користувача;
- країна користувача;
- місто користувача;
- тощо.

Об'єкт:
- таблиця (опціонально, залежить від дії);
- стовпець (опціонально, залежить від дії);
- статус запису (опціонально, залежить від дії);
- власник запису (опціонально, залежить від дії);

Операція:
- назва дії;

Стан:
- день тижня;

- час.

Деякі уточнення стосовно розробленої системи:

- Список атрибутів пов'язаних з суб'єктом може бути розширений будь-якою інформацію (наприклад лімітами на виконання операцій). Для цього необхідно додати новій стовпець в таблицю користувача.

- Дані про таблиці та стовпці необхідні тільки для деяких дій, таких як створення, оновлення, отримання – читання, але не потрібні для, наприклад, такої дії, як кваліфікація інтересу.

- Дії можуть бути як звичайні: створити, видалити, оновити, так і більш складні – кваліфікувати інтерес, експортувати, асоціювати, а також будь-які кастомні дії.

- В доступному для реалізації рішенні немає можливості отримати інші атрибути стану окрім дати та часу, такі як ip-адресу, пристрій, так як вони не містяться в контексті виконання операції.

РОЗРОБКА РІШЕННЯ ДЛЯ ВПРОВАДЖЕННЯ ABAC В CRM СИСТЕМУ

Для впровадження контролю доступу на основі атрибутів для Microsoft Dynamics CRM було розроблено рішення, яке включає такі компоненти як таблиця «ABAC Rules» для зберігання правил з налаштованими в ній полями та формами, плагін, що виконує перевірку правил та кроки плагіну, що забезпечують виконання плагіну при діях в системі. Плагін для кожної дії, для якої виконується, збирає атрибути доступу згідно описаній вище системі атрибутів та виконує перевірку санкціонованості доступу згідно правил.

Якщо результатом перевірки правил буде заборона доступу, то транзакція не буде виконана та якщо дія відбувалася синхронно з'явиться повідомлення «Access denied». Встановлення даного рішення та налаштування даних в таблиці «ABAC Rules» забезпечить дію політики керування доступом на основі атрибутів в системі Microsoft Dynamics CRM. Розробка рішення виконувалася в тріальній версії одного з продуктів Microsoft Dynamics CRM, а саме Microsoft Dynamics 365 Sales, версії 1710 (9.2.21104.142) Online та підходить для встановлення до будь-якої CRM системи на платформі Microsoft Dynamics 365.

ДЕМОНСТРАЦІЯ РОБОТИ РІШЕННЯ

Існує безліч можливих варіантів правил налаштування керування доступом. Для демонстрації роботи рішення для впровадження контролю доступу на основі атрибутів в Microsoft Dynamics CRM було реалізовано декілька з них.

Приклади правил:

1. Записи дзвінка не повинні створюватися після 19.00 та у вихідні дні – суботу та неділю;
2. Користувач на позиції «Junior HR» не повинен здійснювати кваліфікацію інтересу;
3. «Оператор контакт-центру» не може видаляти чи відміняти замовлення, якщо вартість перевищує 50 000 гривень.

Для кожного з цих правил були створені відповідні записи в таблиці «ABAC Rules». (Рис. 1).

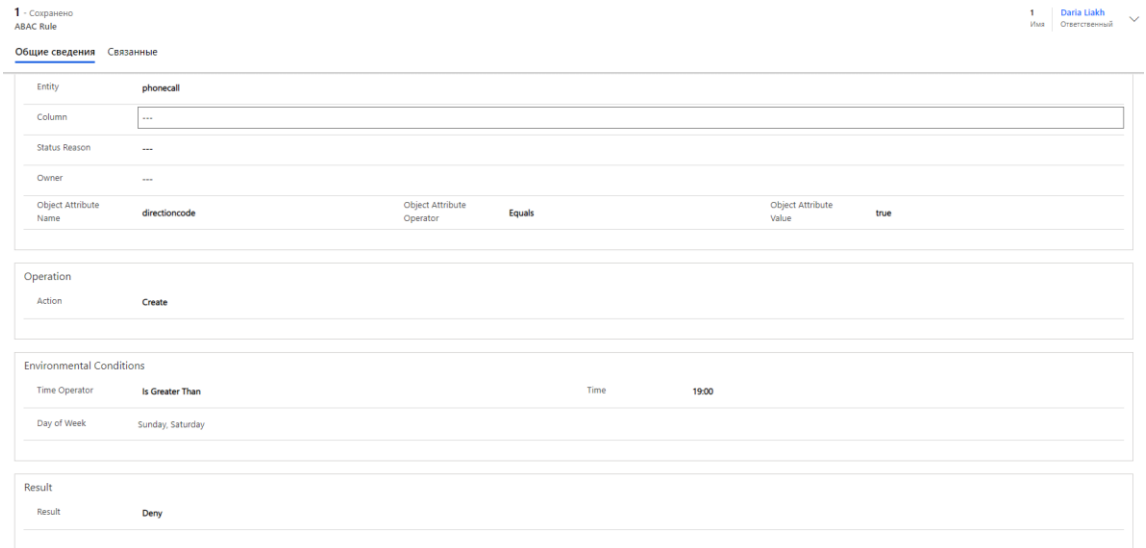

Рис. 1 Скріншот запису першого правила в таблиці «ABAC Rules»

Далі було перевірено результат виконання даних операцій при умовах, за яких згідно політики безпеки запити на виконання операцій повинні бути заборонені. Для першого випадку була здійснена спроба створити запис вихідного дзвінку в системі після 19.00. При натисканні кнопки «Зберегти» створений запис з'явилося повідомлення про помилку та запис не було створено (Рис. 2). Для другого випадку користувач був доданий на позицію «Junior HR» та виконав спробу запустити процес кваліфікації інтересу (створення запису контакту з запису інтересу – потенційного клієнта), проте цей процес так і не був запущений і з'явилося повідомлення про помилку. Для третього випадку користувач був доданий на позицію «Оператор контакт-центру». При спробі видалити чи відмінити замовлення, вартість якого перевищувала 50 000 грн, аналогічно до попередніх двох випадків, дія не була виконана та з'явилося повідомлення. Проте при спробі видалити запис замовлення, вартість якого менше 50000 грн дія була успішно виконана. Отже для даних сценаріїв рішення відпрацювало коректно та згідно вимогам.

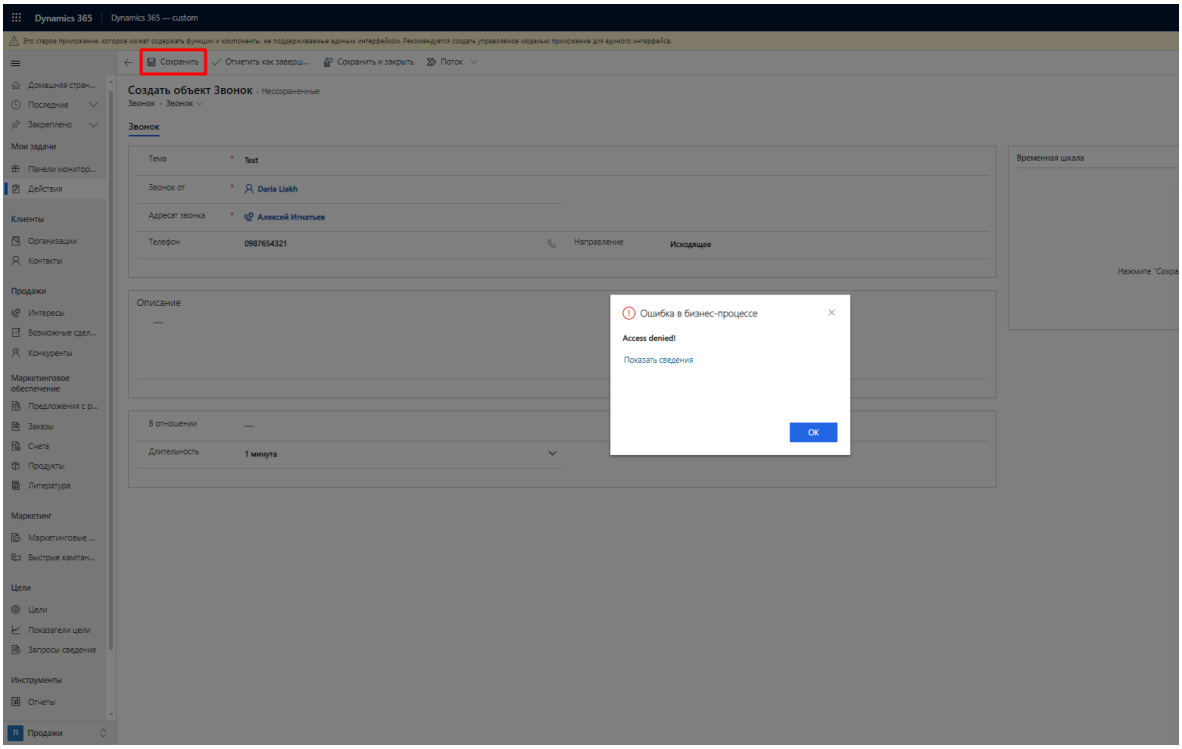

Рис. 2 Скріншот результату спроби створення вихідного виклику у неробочий час

ВИСНОВОК

В даній роботі було досліджено найбільш популярні політики керування доступом. У представлених в роботі системах – Microsoft Dynamics AX та Microsoft Dynamics CRM використовується рольова політика керування доступом з деякими особливостями, описаними вище.

Проаналізувавши системи безпеки даних інформаційних систем класу CRM та ERP було виявлено ряд вимог, які не покривають наявні системи захисту.

Було розроблено власну систему атрибутів специфічну для CRM та ERP систем, яку можна застосувати при реалізації рішення для впровадження системи керування доступом на основі атрибутів для даних інформаційних систем. Було розроблено рішення для впровадження даної системи атрибутів до Microsoft Dynamics CRM та продемонстровано роботу рішення на прикладах.

ЛІТЕРАТУРА

[1] Cleo Team *Understanding the Need for CRM andERP Systems Integration* – https:// www.cleo.com/blog/knowledge-base-erp-and-crm-integration/.

[2] K.Vijayalakshmi, Dr.V.Jayalakshmi *Improving Performance of ABAC Security Policies Validation usinga Novel Clustering Approach.* International Journal of Advanced Computer Science and Applications(IJACSA), Volume 12 Issue 5, 2021. – pp. 245-257.

[3] Neil Madden *API Security in Action*,2020. – 576 p.
[4] *Microsoft Security model concepts* - https:// docs. microsoft.com/en-us/dynamics365/custome re ngagement/on-premises/admin/security-concep ts?view=op-9-1/.
[5] *Microsoft Role-based security* - https://docs. microsoft.com/en-us/dynamics365/fin-ops-core / dev-itpro/sysadmin/role-based-securi ty/ Done Microsoft Dynamics AX -https://done.ua/ rus/ produkti/sistemi-upravli nnya-pidpriemstvom-erp/microsoft-dynamics-ax/.
[6] *NEXTLABS The Definitive Guide to At-tribute-Based Access Control (ABAC)* - https:// www. nextlabs.com/products/technology/abac/.

КОНТРОЛЬ ДОСТУПА НА ОСНОВЕ АТРИБУТОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ КЛАССА CRM И ERP

Эффективное управление процессами в компании в наши дни не обходится без автоматизации. Использование CRM и ERP систем помогает повысить эффективность, автоматизацию и оптимизацию большинства процессов на предприятии. При внедрении CRM или ERP системы каждая компания в обязательном порядке думает об обеспечении безопасности своих данных и, следовательно, об обеспечении четкого и надежного контроля над доступом ко всем данным в системе. В этой статье мы проанализировали две из наиболее распространенных на сегодняшний день политик контроля доступа - политику контроля доступа на основе ролей (RBAC) и политику контроля доступа на основе атрибутов (ABAC). Контроль доступа на основе атрибутов называется будущим контролем доступа, потому что он обеспечивает реализацию сложных политик и зависимость решения о разрешении или запрете доступа не только от роли пользователя, но и от других параметров субъекта, объекта и среды., он предоставляет гораздо больше возможностей для реализации гибких политик контроля доступа. Мы также проанализировали существующие политики контроля доступа ERP-системы - Microsoft Dynamics AX и CRM-системы - Microsoft Dynamics CRM, их особенности. Сформирован ряд требований, которые не покрываются текущей реализацией управления доступом в этих системах, но могут быть удовлетворены политикой управления доступом на основе атрибутов. В ходе работы была разработана собственная система атрибутов, характерная для этих систем, которую можно использовать для разработки решения для реализации политики контроля доступа на основе атрибутов для систем CRM и ERP на платформе Microsoft Dynamics 365. Также было разработано универсальное решение для реализации политики контроля доступа на основе атрибутов для системы Microsoft Dynamics CRM, которая может использоваться как вместо существующей системы контроля доступа на основе ролей, так и вместе для повышения эффективности контроля доступа. система.

Ключевые слова: управление доступом на основе атрибутов (ABAC), управление взаимоотношениями с клиентами (CRM), планирование ресурсов предприятия (ERP).

ATTRIBUTE-BASED ACCESS CONTROL IN CRM AND ERP CLASS INFORMATION SYSTEMS

Efficient process management in a company these days cannot do without automation. Using CRM and ERP systems helps to increase efficiency, automation, and optimization of most of the processes in the enterprise. When implementing a CRM or ERP system, each company mandatory think about ensuring the security of its data and therefore ensuring clear and reliable control over access to all data in the system. In this paper, we analyzed two of the most common access control policies today - the role-based access control policy (RBAC) and the attribute-based access control policy (ABAC). Attribute-based access control is called the future access control because it ensures the implementation of complex policies and the dependence of the decision to allow or deny access not only on the user's role, but also on other parameters of the subject, object, and environment, it provides much more opportunities to implement flexible access control policies. We also analyzed the existing access control policies of the ERP system - Microsoft Dynamics AX and CRM systems - Microsoft Dynamics CRM, their specific features. A number of requirements that are not covered by the current implementation of access control in these systems but can be satisfied by an attribute-based access control policy have been formed. The work has developed its own system of attributes, specific to these systems, which can be used to develop a solution to implement an access control policy based on attributes to CRM and ERP systems on the Microsoft Dynamics 365 platform. A universal solution was also developed to implement an access control policy based on attributes for the Microsoft Dynamics CRM system, which can be used both as a replacement for the existing role-based access control system and also together to improve the efficiency of the access control system.

Keywords: Attribute-based access control (ABAC), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP).

Лях Дар'я Олександрівна, студентка Фізико-технічного інституту КПІ ім. Ігоря Сікорського.
E-mail: daria.liakh@gmail.com.
Orcid ID: 0000-0002-7153-4785.
Лях Дария Александровна, студентка Физико-технического института КПИ им. Игоря Сикорского.
Liakh Daria, student of Institute of Physics and Technologies of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Коломицев Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту КПІ ім. Ігоря Сікорського.
E-mail: box144.85@gmail.com.
Orcid ID: 0000-0001-8460-3041.
Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института КПИ им. Игоря Сикорского.
Kolomytsev Myhailo, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту КПІ ім. Ігоря Сікорського.
E-mail: nos.sv.ol@gmail.com.
Orcid ID: 0000-0002-0016-9346.
Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института КПИ им. Игоря Сикорского.
Nosok Svitlana, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

DOI: 10.18372/2410-7840.23.16407
УДК 004.056:061.68

ЕВРИСТИЧНИЙ МЕТОД ЗНАХОДЖЕННЯ BITSLICED-ОПИСУ ДОВІЛЬНИХ КРИПТОГРАФІЧНИХ S-Box

Ярослав Совин, Іван Опірський, Дмитро Євенко

Bitsliced-підхід до імплементації блокових шифрів поєднує такі переваги як потенційно високу швидкодію, безпеку і невимогливість до обчислювальних ресурсів. Головною проблемою при переході до bitsliced-опису шифру є представлення S-Box мінімальною кількістю логічних операцій. Відомі методи мінімізації логічного опису S-Box мають низку обмежень, наприклад, працюють лише з S-Box невеликих розмірів, є повільними або неефективними, що загалом стримує використання bitsliced-підходу. У роботі запропоновано новий евристичний метод bitsliced-опису довільних криптографічних S-Box та здійснено порівняння його ефективності з існуючими методами на прикладі S-Box шифру DES. Запропонований метод орієнтований на програмну реалізацію в логічному базисі AND, OR, XOR, NOT, що допускає імплементацію з використанням стандартних логічних інструкцій на будь-яких 8/16/32/64-бітних процесорах. Метод використовує низку евристичних технік, таких як, швидкі алгоритми вичерпного пошуку на невелику глибину, гнучку процедуру планування процесу пошуку, пошук в глибину тощо, що в комплексі забезпечують високу ефективність і швидкодію. Це дає змогу адаптувати його для мінімізації 8×8 S-Box, що на сьогодні є дуже актуальним для багатьох блокових шифрів, зокрема вітчизняного шифру «Калина». Запропонований підхід до bitsliced-опису довільних S-Box усуває обмеження відомих методів такого подання, що стримували використання bitcliced-підходу при удосконаленні програмних реалізацій блокових шифрів для широкого кола процесорних архітектур.

Ключові слова: *bitslicing, S-Box, логічна мінімізація, x86-64 CPU, програмна імплементація, блокові шифри.*

ВСТУП

Важливою характеристикою блокових симетричних шифрів (БСШ) є швидкодія, яка у багатьох випадках визначає швидкодію аплікації чи сервісу.

З огляду на різноманіття застосувань БСШ мусить забезпечувати достатньо високу продуктивність для широкого класу мікропроцесорних архітектур із різними обчислювальними можливостями й доступними ресурсами.

Не менш важливою для програмної реалізації БСШ є підвищена стійкість до side-channel атак: для low-end CPU (8/16/32-бітні мікроконтролери) це насамперед атаки аналізу енергоспоживання, для high-end CPU (x86, ARM Cortex-A) це передусім часові та кеш атаки.

Є декілька підходів до програмної реалізації БСШ, що відрізняються швидкодією, безпекою та вимогами до ресурсів: класичний, табличний, на базі SIMD-інструкцій та bitsliced.

З них потенційно найвищою швидкодією володіє bitsliced-підхід, а крім того він забезпечує constant-time імплементацію блокових шифрів з імунітетом до часових та кеш атак [9], є невимогливим до ресурсів, максимально використовує можливості high-end мікропроцесорів щодо збільшення швидкодії внаслідок розпаралелювання як виконання коду (суперскалярність), так і