УДК 004.732

Щербатюк А.В.

ОЦІНКА КРИТЕРІЇВ ВИБОРУ ЕЛЕМЕНТІВ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДЛЯ ПІДПРИЄМСТВ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Вінницький національний технічний університет

Анотація. В даній роботі узагальнено та оцінено критерії оцінки та вибору оптимальної системи контролю доступу для підприємств. Також наведено базові рекомендації з вибору апаратної частини та розробки проекту СКД.

Ключові слова: система контролю доступу, RFID, сканер відбитку пальця, сканер форми обличчя, електронний замок.

Abstract. In this paper, the criteria for evaluating and selecting the optimal access control system for enterprises are summarized and evaluated. Also, the basic recommendations for choosing a hardware component and designing the SKD are given.

Keywords: access control system, RFID, fingerprint scanner, face form scanner, electronic lock.

Вступ

Актуальність теми полягає в тому, що сучасна ситуація в сфері інформаційної безпеки диктує необхідність наявності системи контролю доступу на більшості підприємств малого та середнього бізнесу для захисту інформації та інформаційних систем від несанкціонованого доступу та для блокування спроб несанкціонованого внесення змін до інформаційних систем.

Інформаційні системи присутні на більшості приватних та державних підприємств, оскільки інформація зберігається та обробляється виключно з допомогою електронних засобів, а виведення з ладу серверної частини системи або окремих її елементів з високою вірогідністю блокує роботу підприємства, або принаймні суттєво перешкоджає роботі підприємства в стандартному режимі. Система контролю доступу – система, призначена для обмеження доступу до приміщень, зон та програмних засобів особам, що не мають відповідних повноважень та розмежування прав доступу серед персоналу підприємства.

Мета роботи – оцінити та узагальнити критерії вибору системи контролю доступу для підприємств та сформувати поради для створити короткий список порад для вибору апаратної частини та розробки проекту ефективної системи контролю доступу.

Результати оцінки

Забезпечення інформаційної безпеки підприємства – комплексне завдання, успішне виконання якого залежить від ефективності роботи наступних елементів:

- контроль фізичного доступу до території (контроль автотранспорту та пішоходів);
- авторизація уповноважених осіб під час доступу на територію та доступу до захищених зон;
- контроль доступу до програмного забезпечення, інформаційних ресурсів підприємства, і т.д;

Загалом, типова технічна система контролю доступу складається з наступних елементів:

- пристрій авторизації особи (зчитувач даних, що дозволяють ідентифікувати особу);
- сервер, що обробляє дані, отримані від пристроїв авторизації та зберігає інформацію про час доступу до захищених зон та зберігає інформацію про розмежування прав доступу для авторизованих користувачів;
- пристрій фізичного обмеження доступу (турнікет або електронний замок);

Необхідність авторизації користувачів системи контролю доступу породжує проблему ідентифікації особи для подальшої роботи системи. Ідентифікація може відбуватися з допомогою технології радіочастотних міток (популярні стандарти – MIFARE, E-MARINE), відбитків пальців (одного або декількох), з допомогою електронних ключів на будь-яких носіях, з допомогою сканування інших унікальних параметрів людського тіла: форми обличчя, сітківки ока, форми вух, носа, або розрізу очей.

Станом на сьогоднішній день, технології біометричної ідентифікації людини (окрім сканування відбитків пальців) є надзвичайно дорогими та встановлення подібних систем на підприємствах малого та середнього бізнесу може бути недоцільним через те, що вартість системи контролю доступу наближується до вартості інформації, що обробляється чи зберігається на підприємстві. Тому доцільним є введення системи радіочастотних міток (RFID – Radio Frequency IDentification) та сканування відбитків пальців. Вищеописані технології забезпечують надійну ідентифікацію персон, а їх комбінація дозволяє забезпечити ідентифікацію також тих осіб, що мають проблеми з ідентифікацією через відбитки пальців (до них відносяться ті люди, чиї руки постійно контактують з водою, хімічними речовинами, мастилами та абразивами – майстри-верстатники, прибиральники, посудомийними, монтери).

Після ідентифікації особи постає проблема розмежування прав доступу, що задані адміністратором політики безпеки згідно завдань та обов'язків, що покладені на ідентифіковану особу. Дані про рівні доступу та про час ідентифікації та надання доступу обробляються та зберігаються на сервері. Сервер системи контролю доступу – віддалений комп'ютер, на якому встановлене відповідне програмне забезпечення та на якому зберігається база даних користувачів системи. Сучасні системи контролю доступу дозволяють використовувати в якості сервера будь-який комп'ютер з мінімальними характеристиками. Основні вимоги до сервера:

- надійність роботи;
- наявність відповідних портів для передачі даних до сканеру(-ів) та пристроїв фізичного обмеження доступу. Найчастіше для цього використовується порт Ethernet;

Загалом, виходячи з вищеописаних досліджень, сформовано список порад з вибору елементів системи контролю доступу для невеликих підприємств:

- використання зчитувачів радіочастотних міток та сканерів відбитків пальців середнього цінового діапазону;
- використання бюджетного комп'ютера в якості сервера системи контролю доступу;
- використання джерел безперебійного живлення для забезпечення роботи системи у випадку відключення живлення від мережі;
- використання електронних замків на дверях приміщень контрольованих зон.

Висновки

В даній роботі було проведено оцінку існуючих технічних елементів сучасних бюджетних систем контролю доступу (СКД), проведено оцінку технологій та методів ідентифікації користувачів системи для надання відповідних повноважень, проаналізовано існуючі сучасні системи розмежування доступу та розраховане для них оптимальне співвідношення «вартість системи / рівень захисту» для визначення економічної доцільності використання відповідних елементів СКД для малих та середніх підприємств.

Також було наведено базові загальні поради для вибору елементів систем фізичного контролю доступу для бюджетних СКД, використання яких забезпечує оптимальний рівень захисту приміщень та обладнання від несанкціонованого доступу.

Було розроблено мінімальні рекомендації для майбутніх адміністраторів систем інформаційної безпеки щодо розмежування прав доступу авторизованих користувачів на підприємствах для забезпечення комфортного користування системою для користувачів всіх рівнів доступу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В. Подлазов, В. Борисенко, С. Юдицкий.Узкие места в локальных сетях [Електронний ресурс]. - Режим доступу: http://www.osp.ru/lan/1998/09/133684/

2. Киселев Г.Д., Шпакаускас М.С. Мониторинг мультисервисных компьютерных сетей средствами системы Nagios // Электроника и связь. Тематический выпуск «Электроника и нанотехнологии». 2017 – С. 18-49.

3. Выбор параметров контроля технического состояния для цифровых блоков корпоративной сети на основе использования методов факторного анализа. / Г.С. Петриченко, Л.Н. Дудник // Межотраслевой научно- технический журнал «Автоматизация и современные технологии» – М: Машиностроение – 2010 – №2, С.16-21.

4. Репозиторій контролера ТМО [Електронний ресурс]. - Режим доступу: https://github.com/itmo-infocom/ (дата звернення: 13.06.2013).

5. CPqD/of12softswitch [Електронний ресурс]. - Режим доступу: https://github.com/CPqD/of12softswitch

Щербатюк Артем Володимирович – студент групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький Національний Технічний Університет, Вінниця, e-mail: artemmaitek@gmail.com.

Artem Shcherbatyuk – student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, Ukraine, e-mail: artemmaitek@gmail.com