УДК 621.3.049.77–048.24:537.2

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ И СПОСОБЫ ЕЕ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Никанав М.Ю.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Вышинский Н.В. – канд.техн.наук, профессор, профессор кафедры ИКГ

Аннотация. Рассмотрены технологические возможности использования двухфакторной аутентификации. Рассмотрены проблемы, существующие в сфере безопасности и систем контроля и управления доступом. Проанализированы преимущества и недостатки систем контроля и управления доступом с различными методами аутентификации пользователя. Предложен метод использования двухфакторной аутентификации в системе контроля и управления доступом.

Ключевые слова: аутентификация, идентификация, система контроля и управления доступом

Введение. Сегодня как никогда остро стоит вопрос защиты информации. Одним из самых простых и в тоже время надёжных способов обеспечения сохранности интеллектуальной собственности является система контроля и управления доступом (СКУД). Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом будет система контроля и управления доступом на объект. Хорошо организованная, с использованием современных технических средств СКУД позволит решать целый ряд задач.

Двухфакторная аутентификация уместна в абсолютном большинстве точек контроля доступа СКУД. Мало применима она лишь в случаях, когда критическое значение имеет время авторизации, и любое замедление этого процесса ведет к серьезным неудобствам – например, контроль доступа через турникет на проходных заводах.

Двухфакторная аутентификация, несомненно, повышает надежность систем, ведь вероятность случайного совпадения данных по двум методам значительно уменьшается. Это справедливо относительно решений, ключом к которым является лишь один метод.

Основная часть. Одними из основных средств защиты информационных систем от постороннего вмешательства являются идентификация и аутентификация. Аутентификация и идентификация пользователя являются взаимозависимыми действиями распознавания и проверки подлинности.

Аутентификация – процедура проверки подлинности. Основной целью аутентификации пользователя информационной системы является снижение угроз безопасности, а именно нарушение конфиденциальности и целостности информации. Несанкционированный доступ – один из самых распространенных видов нарушений, представляющий непосредственную угрозу работоспособности системы [1].

Аутентификация используется не только для доступа к социальным сетям, электронной почте, интернет-магазинам, платежным системам, но и в различных системах контроля и управления доступом.

Аутентификация пользователя в системе контроля и управления доступом классифицируется по следующим типам:

– аутентификация на основе пароля;
– аутентификация по смарт-карте;
– биометрическая аутентификация.

Аутентификация на основе пароля. Идентификация пользователя проводится по одноразовым и многоразовым паролям. Многоразовый пароль задает пользователь, а система хранит его в базе данных. Он является одинаковым для каждой сессии. К ним относятся PIN–коды, слова, цифры, графические ключи. Одноразовые пароли для каждой сессии являются разными.

Преимущества. Одна из сильных сторон заключается в том, что более длинный пароль очень трудно взломать. На этапе использования паролей крайне важно использовать надежные пароли. Надежный секретный ключ состоит из заглавных букв, строчных букв, цифр и уникальных символов. Теперь администраторы безопасности рекомендуют пароли из 12 символов. Для взлома пароля из 12 символов потребуется 55 дней с использованием суперкомпьютеров.

Недостатки. Возможность подслушивания пароля является большой проблемой. Злоумышленник может узнать пароль на разных этапах общения. Даже если пароль надежный, он может быть получен злоумышленником. Ключевая проблема с именем пользователя и паролем - человеческий фактор:

- пароль легко угадать или выполнить поиск, если пароль легкий;
- пароль легко украсть, если он записан;
- пользователи могут обмениваться паролями;
- пароль может быть забыт, если он сложный.

Аутентификация по смарт-карте. Для идентификации пользователю необходимо обладать физическим объектом, смарт-картой, чтобы получить доступ. Смарт-карта - это карта, по размеру аналогичная кредитной карте, со встроенным цифровым сертификатом для идентификации владельца [2].

Преимущества. Одним из главных преимуществ смарт-карты является то, что она хранит в себе информацию о пользователе. Благодаря данной информации можно отслеживать передвижение пользователя по территории, время прибытия и убытия. Неоспоримым преимуществом является то, что в отличии от аутентификации на основе пароля пользователю не нужно запоминать сложную комбинацию, необходимо лишь обладать физическим объектом, смарт-картой.

Недостатки. Главным недостатком смарт-карты является то, что она является физическим объектом, а значит может быть украдена.

Биометрическая аутентификация. Предотвращает утечку или кражу персональной информации. Проверка проходит по физиологическим характеристикам пользователя, например, по отпечатку пальца, сетчатке глаза, распознавание лица и тембру голоса.

Преимущества. Основные преимущества биометрической аутентификации:

- не требуется запоминание пароля;
- биометрия уникальна;
- очень трудно воспроизвести биометрическую функцию;
- биометрические характеристики не могут быть потеряны.

Недостатки:

- логические ошибки;
- ошибки ложного принятия;
- настройки точности;
- невозможность сканирования при получении травмы.

Согласно статистике компании *InfoWatch*, количество утечек данных в мире беспрерывно растет, за первую половину 2022 года 2101 случай утечки конфиденциальной информации – что почти в 2 раза (на 93,2%) больше, чем за аналогичный период 2021 года. Количество утечек в России за первое полугодие 2022 года составило 305, что на 45,9% больше, чем за аналогичный период 2021 года (рисунок 1).

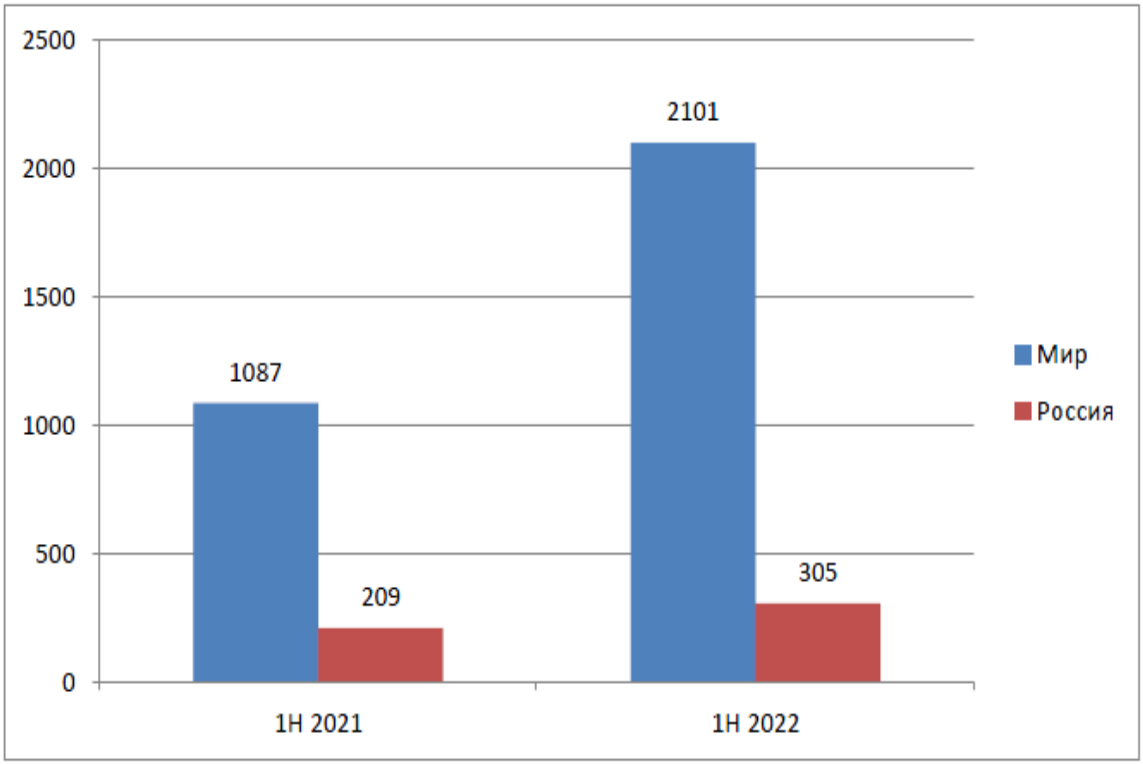

Рисунок 1 – Статистика числа утечек Мир-Россия за 2021 и 2022 года

Объемы скомпрометированных данных растут из-за увеличения мощности внешних и внутренних утечек. При этом утечки по всем каналам, кроме сетевых, зачастую просто не фиксируются.

Таким образом, возникает проблема защиты конфиденциальной информации от атак злоумышленников. Одним из средств защиты информации является парольная защита с использованием второго фактора.

Предлагаемый подход. Современные СКУД — это сложные, многокомпонентные системы. Тем не менее, главная задача СКУД на протяжении десятков лет остается неизменной: обеспечить автоматический проход на объект людей, имеющих такое право [3].

СКУД можно определить как систему обеспечения нормативных, организационных и материальных гарантий выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию и как совокупность организационно-правовых ограничений и правил, устанавливающих порядок пропуска сотрудников объекта, посетителей, транспорта ввоза/вывоза материальных ценностей.

Предлагаемый подход строится на основе значительного повышения безопасности объекта, одним из ключевых процессов которой является двухфакторная аутентификация. На основе приведенных преимуществ и недостатков методов аутентификации можно сделать вывод, что наиболее оптимальным будет использование аутентификации на основе пароля в совокупности с аутентификацией по смарт-карте. Структурная схема устройства представлена на рисунке 2.

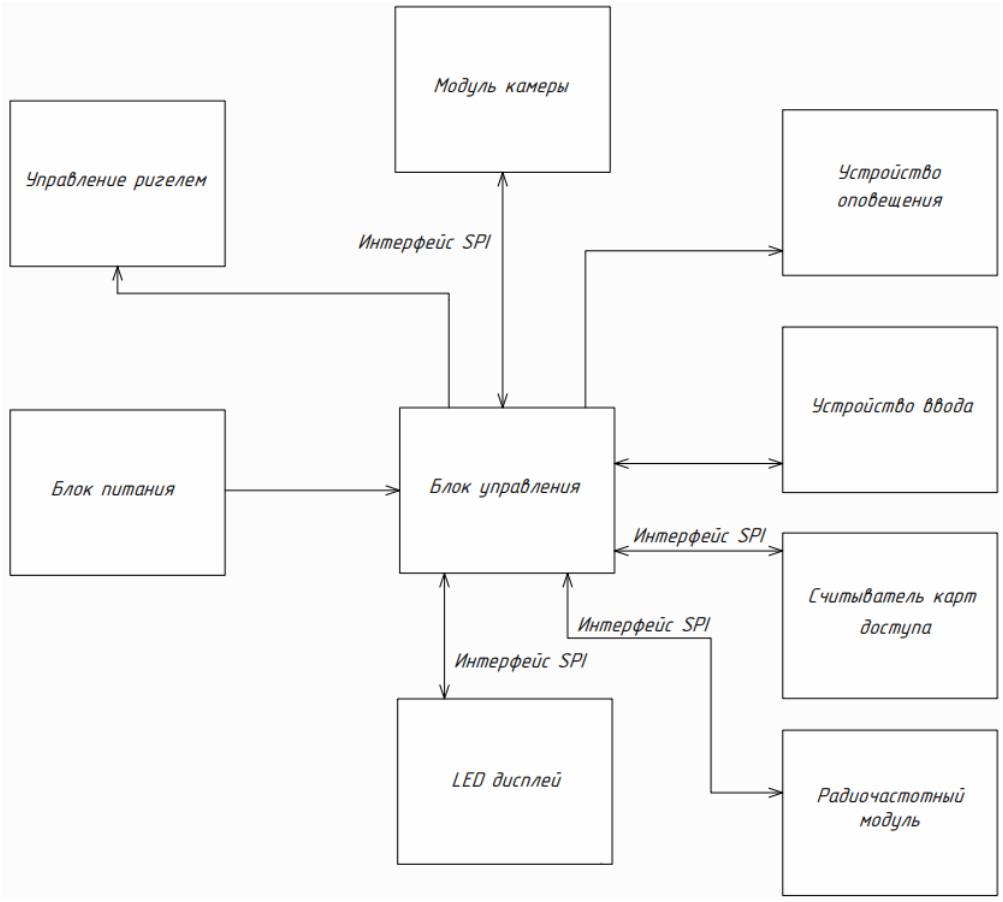

Рисунок 2 – Структурная схема системы контроля и управления доступом на основе двухфакторной аутентификации

Алгоритм работы устройства представлен на рисунке 3. Для срабатывания замкового механизма необходимо к считывающему устройству поднести специальную карту-идентификатор, на которой содержится уникальный код с уровнем доступа носителя. Далее на основе полученной информации принимается решение о разрешении или запрете доступа к объекту.

В случае положительного ответа, активируется клавиатура, на которой нужно ввести PIN-код. Если PIN-код соответствует коду, хранящемуся в памяти микроконтроллера, то срабатывает электромеханическое устройство, и замок открывается. Одновременно с этим должен сработать звуковой сигнал, который сориентирует пользователя о решении системы, одновременно с ним должна сработать световая индикация. Зеленый светодиод поможет пользователю быстрее отреагировать на решение системы. Аналогичный алгоритм действий и при отказе. Он должен сопровождаться соответствующим звуковым сигналом.

Для того, чтобы выйти из помещения, необходимо воспользоваться специальной кнопкой. После её нажатия автоматически сработает замковой механизм и откроет дверь.

Отличительной характеристикой данной системы является разграничение уровней доступа, а также система двухфакторной аутентификации, что значительно повышает безопасность объекта.

На основе полученных данных система принимает решение о допуске. При трехкратном неправильном введении кода срабатывает соответствующая звуковая сигнализация и включается камера.

При разрешении доступа происходит отпирание замкового механизма, открывается дверь. После закрытия двери замковой механизм возвращается в исходное состояние.

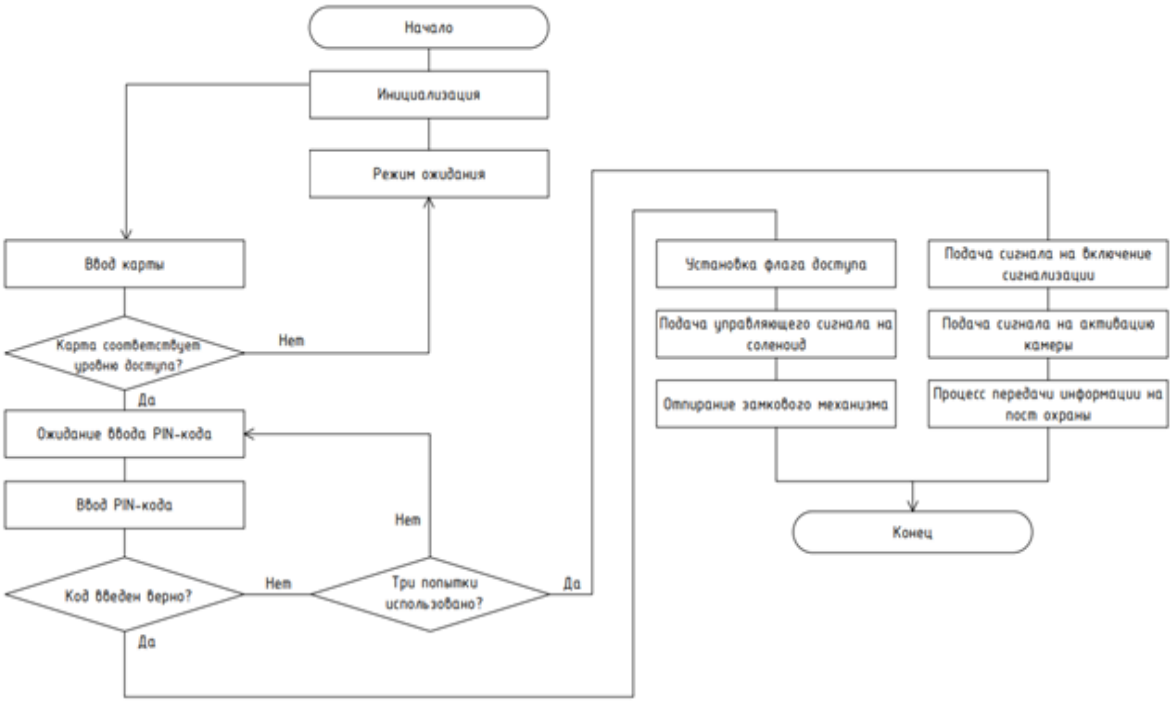

Рисунок 3 – Алгоритм работы системы контроля и управления доступом на основе двухфакторной аутентификации

Заключение. Система контроля и управления доступом, основывающаяся на двухфакторной аутентификации, позволяет обеспечить нормативные, организационные и материальные гарантии выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность.

Список литературы

1. *Аутентификация [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Аутентификация - Дата доступа : 10.02.2023.*

2. *Farik. M. A Review Of Authentication Methods / M. Farik // International Journal of Scientific & Technology Research / 2016. P. 246-249.*

3. *Шишкин, С. Кодовый замок с загрузкой эталонного кода по RS-485 / С. Шишкин // Современная электроника. - 2015. - №2: С.46-49.*

UDC 621.3.049.77–048.24:537.2

TWO-FACTOR AUTHENTICATION AND WAYS TO USE IT IN ACCESS CONTROL AND MANAGEMENT SYSTEMS

Nikanau M.U.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vyshinski N.V. - PhD, full professor, professor of the Department of ECG

Annotation. The technological possibilities of using two-factor authentication are considered. The problems existing in the field of security and access control and management systems are considered. The advantages and disadvantages of access control and management systems with various methods of user authentication are analyzed. A method of using two-factor authentication in the access control and management system is proposed.

Keywords: authentication, identification, access control and management system.