DOI: 10.17117/na.2016.09.01.389

<http://ucom.ru/doc/na.2016.09.01.389.pdf>

Поступила (Received): 24.09.2016

Глотова И.О., Суханов С.В.
Способ повышения защиты информации в АСУ
коммерческого предприятия

Glotova I.O., Sukhanov S.V.
A method for improving information security in ACS of business

В статье рассматривается структура АСУ предприятия и проблема связанная с несанкционированным доступом к данным. Предложено решение поставленной проблемы с помощью применения физически неклонируемых функций. Разработаны алгоритмы, реализующие предлагаемые пути решения проблемы

Ключевые слова: АСУ, физически неклонируемые функции, аутентификация

The article describes the structure of ACS the enterprise and problems associated with unauthorized access to the data. Proposed solution to the problem through the use of physically Nonclonability functions. Proposed the algorithms that implement solutions to the problem

Key words: ACS, physical unclonable functions, authentication

Глотова Ирина Олеговна

Студент

Московский авиационный институт
г. Москва, Волоколамское шоссе, 4

Glotova Irina Olegovna

Student

Moscow aviation institute
Moscow, Volokolamskoe highway, 4

Суханов Семён Валерьевич

Преподаватель

Московский авиационный институт
г. Москва, Волоколамское шоссе, 4

Sukhanov Semen Valerievich

Teacher

Moscow aviation institute
Moscow, Volokolamskoe highway, 4

Введение. В настоящее время представить нашу жизнь без автоматизированных систем управления (АСУ) достаточно сложно. Зачастую они отвечают за обработку критически важной информации. Так, АСУ технологическим процессом (ТП) поддерживают процессы управления технологическим объектом, нарушение которых может привести к техногенным авариям, угрожающим жизни людей. Безопасность ТП в общем смысле – это, прежде всего, безопасность для жизни и здоровья людей и окружающей среды. Поэтому вопросы обеспечения правильного функционирования АСУ становятся всё актуальнее.

Проблема. Структура АСУ является реализацией соответствующего принципа управления. Принципы управления – это основные правила, определяющие функционирование системы, а также – важнейшие требования, соблюдение которых обеспечивает эффективность управления [1]. В современных системах управления существуют различные принципы управления, но одним из самых распространенным является именно иерархический.

Иерархическая структура предполагает декомпозицию задачи управления. Таким образом, функцию управления разделяют между различными соподчиненными частями системы – уровнями. Каждому уровню делегируются строго определенные полномочия и ставятся конкретные задачи. При этом вышестоящий уровень управляет нижестоящими. Таким образом сверху вниз поступают команды управления, а снизу вверх – донесения о получении команды и ее выполнении. Такие разграничения могут служить причиной нарушения целостности и конфиденциальности информации. Поэтому зачастую защищать автоматизированную систему приходится не только от злоумышленников извне, но и от действий самих сотрудников.

Анализ существующих путей решения

Самыми распространёнными способами защиты информации, циркулирующей в системе, являются идентификация, аутентификация и авторизация пользователей (сотрудников).

Аутентификация пользователя – это проверка того, действительно ли пользователь является тем, за кого себя выдает. Аутентификация в том или ином виде необходима всем системам, в которых предусматривается какое-либо ограничение и разграничение доступа к данным.

Для корректного проведения процедуры аутентификации пользователя необходимо, чтобы тот предоставил аутентификационную информацию – некие уникальные данные, которыми должен обладать только он и никто другой.

Сама процедура аутентификации в общем случае выполняется в два следующих этапа:

1. У пользователя однократно запрашивается некий эталонный образец аутентификационной информации, например, запрашивается пароль. Данный образец хранится у субъекта системы, проверяющего аутентификацию – модуля аутентификации (например, сервера, который запрашивает аутентификацию пользователей). Обычно время действия данного эталона ограничено, и по истечению срока эталонный образец запрашивается снова.

2. Каждый раз при выполнении аутентификации у пользователя запрашивается аутентификационная информация, которая сравнивается с эталоном. На основе данного сравнения делается вывод о подлинности пользователя.

В случае удаленной аутентификации существует проблема передачи аутентификационной информации по каналам связи, которые могут быть небезопасны (через Интернет или локальную сеть). Чтобы уникальная информация не была раскрыта, при пересылке по таким каналам используется множество протоколов аутентификации. Однако большим недостатком существующих протоколов является открытость их алгоритмов работы. Таким образом, зная используемый протокол аутентификации, злоумышленник может осуществить различные виды атак на него [2].

Для борьбы с вышеуказанной проблемой авторами предложен подход, основанный на применении физически неклонируемых функций (ФНФ). ФНФ – это физические системы, неотъемлемым свойством которых является неклонируемость (неповторяемость) некоторых их функций, свойств, характеристик

либо параметров. При производстве микросхем, они подвергаются воздействию внешней среды (незначительное изменение температуры, давления, вибрации), что влечет за собой неконтролируемое изменение в физической структуре (небольшое изменение толщины токопроводящих дорожек, шероховатость поверхности). Совокупность этих изменений формирует уникальный и неклонируемый отпечаток микросхемы (сравнимый с отпечатком пальца человека). Таким образом, по своей природе все микросхемы уникальны [5]. Для снятия отпечатка микросхемы существуют различные конструкции ФНФ [3], которые реализуются на программируемых логических интегральных схемах (ПЛИС) или на статическом ОЗУ (СОЗУ) микросхемы. В данной статье приведен алгоритм аутентификации на основе ФНФ СОЗУ [4].

СОЗУ широко используются в вычислительной технике для хранения данных. Ячейка данного устройства всегда находится в одном из двух состояний, что, в свою очередь, позволяет использовать ее для хранения одного бита информации. При этом СОЗУ является энергозависимой памятью, которая сбрасывается при отключении питания. На этом и основан основной принцип работы ФНФ СОЗУ. При подаче питания на микросхему ячейки СОЗУ инициализируются случайными двоичными значениями, которые формируют её отпечаток. Таким образом, зная отпечатки ста одинаковых СОЗУ микросхем невозможно предугадать отпечаток 101-ой микросхемы.

Предполагаемое решение

С учетом вышеизложенного ФНФ будет использоваться в качестве генератора ключа, который применяется в процедуре аутентификации. Микросхема с СОЗУ должна быть интегрирована на ЭВМ каждого сотрудника, желающего работать в системе. Предлагаемая методика состоит из трех алгоритмов:

- 1) алгоритм формирования секретного пароля;
- 2) алгоритм регистрации;
- 3) алгоритм аутентификации.

Алгоритм формирования секретного пароля состоит из следующих шагов:

- 1) пользователь производит ввод пароля с клавиатуры;
- 2) шифрование введенного пароля на ключе, сформированного ФНФ СОЗУ;
- 3) (необязательный шаг) хэширование зашифрованной последовательности.

Алгоритм регистрации:

- 1) при первичной регистрации пользователь вводит свой идентификатор (логин) и пароль;
- 2) формируется секретный пароль, который вместе с идентификатором отправляется на сервер;
- 3) полученные сервером данные сохраняются в базе.

Алгоритм аутентификации:

- 1) пользователь вводит свой идентификатор и пароль;
- 2) формируется секретный пароль, который вместе с идентификатором отправляется на сервер;

3) на сервере происходит извлечение из базы секретного пароля, соответствующего полученному логину. Далее происходит сравнение полученного секретного пароля и извлеченного из базы. В случае их совпадения пользователь проходит аутентификацию и получает соответствующий доступ.

Таким образом, основными достоинствами разработанной методики АСУ являются:

1) зная атрибуты пользователя АРМ, злоумышленник не сможет работать в системе;

2) неклонировуемость ФНФ исключает создание идентичного АРМ.

К недостаткам можно отнести тот факт, что на каждую ЭВМ, с которой предполагается вход и дальнейшая работа в автоматизированной системе, должна быть оснащена своей ФНФ. Это ведет к некоторым финансовым затратам.

Список используемых источников:

1. Давлетханов М. Концепция одноразовых паролей в системе аутентификации // ВУТЕ. 2006. №7-8 (95). С. 21-25.
2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.
3. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонлируемые функции // Информатика. 2011. №2. С. 92-103.
4. Maes R., Tuyls P., Verbauwhede I. Intrinsic PUFs from Flip-flops on Reconfigurable Devices // WISSec. Eindhoven, 2008. P. 3-20.
5. Pappu R.S., Recht B., Taylor J., Gershenfeld N. Physical One-Way Functions // Scienc. 2003. №297. P. 2026-2030.

© 2016, Глотова И.О., Суханов С.В.

Способ повышения защиты информации в АСУ
коммерческого предприятия

© 2016, Glotova I.O., Sukhanov S.V.

A method for improving information security in ACS of
business