СИГОВ Д. Е., КОЛЕСОВ Д. М. СИСТЕМА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ УРОВНЯ ЦЕНТРАЛЬНОГО ДИСПЕТЧЕРСКОГО ПУНКТА ООО «ГАЗПРОМ ТРАНСГАЗ УХТА»

УДК 004.62:65.011.56, ВАК 05.13.19, ГРНТИ 81.93.29

Система двухфакторной аутентификации пользователей системы диспетчерского управления (СДУ) уровня центрального диспетчерского пункта (ЦДП) ООО «Газпром трансгаз Ухта»

Д. Е. Сигов, Д. М. Колесов

ООО «Газпром трансгаз Ухта», г. Ухта

В статье рассматриваются проблемы информационной безопасности, причины отказа пользователей от использования системой двухфакторной аутентификации в СДУ, проблемы простых и сложных паролей, а также причины компрометации паролей пользователей.

Ключевые слова: *двухфакторная аутентификация, 2FA, информационная безопасность.*

Two-factor user authentication system of dispatching control (CDS) level of Central control station (MCS), LLC “Gazprom transgaz Ukhta”

D. E. Sigov, D. M. Kolesov

ООО «Газпром трансгаз Ухта», Ukhta

In the article the problems of information security, the causes of failure of the users from system use two-factor authentication in CAS, the problems of simple and complex passwords, as well as the reasons for the compromise of user passwords.

Keywords: *two-factor authentication, 2FA, it security.*

Введение

Одной из главных проблем потеря доступа или несанкционированного доступа к любой системе, к сожалению, является человеческий фактор. Пользователи выбирают короткие и простые пароли, которые легко запомнить, но легко подобрать [1]. А длинные и сложные трудно взломать, но запомнить непросто. Чтобы не утруждать себя запоминанию сложных паролей, пользователи записывают эти важные сведения, например, в блокнот, на стикер, который затем закрепляется на монитор или прячется под клавиатурой. Зная традицию обращения

с такими данными работниками российских предприятий, с помощью социальной инженерии злоумышленнику не составит труда получить эти сведения, что приводит к несанкционированным доступам или к более тяжёлым последствиям.

Социальная инженерия – это метод управления действиями человека без использования технических средств.

Ещё одной существенной угрозой информационной безопасности является инсайдинг. Инсайдинг заключается в потенциальной возможности физического доступа злоумышленника к рабочей станции легального пользователя и передача конфиденциальной информации третьим лицам.

Во избежание тяжёлых последствий от несанкционированных доступов, предприятием было принято решение внедрить дополнительный уровень безопасности СДУ, а именно систему двухфакторной аутентификации.

Дфухфакторная аутентификация – это метод идентификации пользователя при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.

Типами аутентификационных данных является [2]:

1. знание – информация, которую знает субъект;
2. владение – вещь, которой обладает субъект;
3. свойство, которым обладает субъект.

Недостатки «старой» системы двухфакторной аутентификации

На данный момент внедрённая система двухфакторной аутентификации пользователей СДУ имеет ряд существенных недостатков. А именно:

1. Пользователь «жёстко» привязан к одному АРМ. Из-за того, что на смарт-карту записывается сертификат локального профиля пользователя, пользователь может иметь доступ к СДУ только на своём АРМ. Чтобы иметь доступ на другом АРМ пользователю нужно на каждом АРМ создавать свои локальные профили, что в итоге создаются неудобства в работе самого пользователя.

2. Смена основного пароля пользователя приводит к ошибке аутентификации. Если пользователь, зашедший в систему с помощью основного пароля, решит обновить пароль, как того требует политика информационной безопасности, то при следующей аутентификации с помощью смарт-карты пользователь не сможет получить доступ к СДУ.

3. Невозможно удалённо заблокировать доступ к СДУ. Если системному администратору показалось, что смар-картой завладел злоумышленник и PIN-код смарт-карты был скомпрометирован, то в целях обеспечения информационной безопасности СДУ системный администратор не может удалённо заблокировать доступ из-за отсутствия центрального пункта управления сертификатами.

4. Сложность подготовки смарт-карты. Трудность заключается в том, что не все пользователи умеют осуществлять запись сертификата локального профиля пользователя на смарт-карту с помощью специального ПО.

Данные недостатки спровоцировали отказ пользователей использовать данную систему аутентификации, как основную, перейдя на классическую защиту. Что привило к проблемам, которые описаны в абзаце «Введение». В связи с этим

необходимо разработать систему двухфакторной аутентификации пользователей СДУ, которая будет лишена данных недостатков.

Аналоги

Были рассмотрены аналоги на мировом и российском рынке. Каждая компания предлагала свои решения в области информационной безопасности. Из них выделялись решения таких компаний, как «Актив» и «Indeed Identity»

Компания «Актив» в качестве клиентского ПО предлагает использовать «Рутокен KeyBox». Это средства администрирования и управления жизненным циклом ключевых носителей (USB-токенов, смарт-карт и других устройств), ориентированное на использование в корпоративных сетях, построенных на технологиях Microsoft Windows. Рутокен KeyBox является системой, обеспечивающей связь между учётными записями пользователей, средствами аутентификации, приложениями и регламентами информационной безопасности. А На основе рутокена для Windows позволяет за короткий срок внедрить аппаратную аутентификацию пользователей и защиту электронной переписки в сетях на базе Microsoft Windows Server. Решение построено на применении встроенных инструментов безопасности Windows и электронных идентификаторов семейства Рутокен в качестве носителей ключевых информации.

В качестве основного решения молодая компания «Indeed Identity» предлагает «Indeed enterprise authentication». Это полноценная платформа, которая позволяет пройти строгую и усиленную аутентификацию с помощью смарт-карты и USB-ключей любых производителей, биометрией, RFID-картой. Производить журналирование действий администраторов и пользователей. Также позволяет реализовать различные сценарии многофакторной аутентификации пользователей. Все поддерживаемые технологии можно комбинировать между собой, например, можно аутентифицировать пользователей по отпечатку пальца и бесконтактной карте, смарт-карте и OTP и др.

Но так как предприятие имеет в наличии смарт-карт ридеры и смарт-карты компании «Аладдин Р. Д.» и у пользователей имеется опыт работы с ПО eToken PKI Client Properties, которое позволяет администрировать и управлять жизненным циклом смарт-карты, было принято решение использовать данные средства в «новой» системе двухфакторной аутентификации пользователей СДУ.

Результаты

Результатом является реализация системы двухфакторной аутентификации пользователей СДУ без рассмотренных недостатков. Данная система протестирована пользователями СДУ, что позволило внедрить данную систему в эксплуатацию и использовать эту систему, как основную систему аутентификации пользователей СДУ. В связи с этим уменьшился риск компрометации пароля пользователя.

Достичь такого результата позволило размещение центра сертификации в сети АСУ ТП предприятия, где размещена СДУ. Центр сертификации позволяет пользователям удалённо запрашивать сертификаты для дальнейшего использования и в автоматическом режиме производить запись сертификата на смарт-

карту. Это лишает необходимости пользователям обращаться за помощью к системному администратору. А системному администратору дана возможность удалённо блокировать доступ к СДУ пользователям, у которых компрометирована ключевая информация.

Выводы

Обеспечить безопасность процесса аутентификации в СДУ критически важно. Двухфакторная аутентификация может применяться не только для целей собственно аутентификации. Важным преимуществом, которое даёт двухфакторная аутентификация, это уникальность пользователя. Это обеспечивается с помощью невозможности «размножения» аутентификационной информации. Логин и пароль пользователя могут использовать сколько угодно людей. А благодаря смарт-карте, воспользоваться ключевой информацией станет возможно только для одного человека – обладателя смарт-карты.

Кроме того, рассмотрена перспектива развития данной системы. А именно расширение возможностей данной системы и возможность интеграции с системой бюро пропусков, которая основана на технологии RFID. RFID – это технология автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в RFID – метках [3]. И у сотрудников предприятия будет единая карта. Карта, которая будет позволять пройти аутентификацию не только в СДУ, но и в других системах предприятия и давать проходить любые контрольно-пропускные пункты предприятия.

Список литературы

1. СТО 74.90-00159025-001-2016. Политика информационной безопасности автоматизированной системы управления технологическими процессами.

2. Многофакторная аутентификация [Электронный ресурс] // Википедия свободная энциклопедия. Режим доступа: https://ru.wikipedia.org/wiki/Многофакторная_аутентификация.

3. Взгляд изнутри: RFID и другие метки [Электронный ресурс] // Хабрахабр. Режим доступа: https://habrahabr.ru/post/161401.

List of references

1. STO 74.90-00159025-001-2016. The policy of information security of automated control system of technological processes.

2. “Multifactor authentication”, *Wikipedia the free encyclopedia*. Mode of access: https://ru.wikipedia.org/wiki/Многофакторная_аутентификация.

3. “An inside look: RFID and other labels”, *Habrahabr*. Mode of access: https://habrahabr.ru/post/161401.