Thus, the obtained results allow to estimate the level of information security of the automated production management system for high-speed distributed data transmission paths.

Анализ методов цифровой аутентификации

УДК 004.056.53

Юрий Журов

Национальный авиационный университет, iurii.zhurov@gmail.com

В течение первых двух десятилетий XXI века количество информационных систем (ИС) увеличилось на несколько порядков, также увеличилось количество субъектов ИС, а также плотность использования ИС одним субъектом. Особо стоит отметить возросшее количество взаимодействий объектов ИС. Данный тренд имеет резко положительную динамику и, так как, каждое взаимодействие субъектов/объектов ИС должно быть аутентифицировано, удерживается постоянный высокий запрос на: 1) эффективные экономически; 2) имеющие высокую степень надежности с точки зрения информационной безопасности; 3) эффективные с точки зрения внедрения; 4) производительные – методы или системы цифровой аутентификации.

Цель данной работы заключается в анализе существующих методов цифровой аутентификации для определения возможных направлений развития научного и практического поиска.

Рассмотрим классические методы аутентификации – методы, основанные на использовании, так называемых, факторов аутентификации. Выделяют следующие факторы – 1) знания; 2) владения; 3) свойства. Эмпирически все доступные варианты верификации аутентифицируемого субъекта/объекта можно отнести к одной из этих категорий, поэтому текущие методы базируются либо на использование этих факторов, либо на мультипликации факторов или вариативности их использования. Такими методами являются 1) однофакторная аутентификация (SFA); 2) двухфакторная аутентификация (2FA); 3) многофакторная аутентификация (MFA).

В 2005 году Shintaro Mizuno, Kohji Yamada, Kenji Takahashi на конференции Proceedings of the 2005 Workshop on Digital Identity Management в докладе «Authentication using multiple communication channels» предложили метод аутентификации с использованием нескольких коммуникационных каналов (МСА), однако общее состояние развития ИС и коммуникационных каналов на 2005 год не позволило выделить данный метод в отдельный подход цифровой аутентификации и МСА принято рассматривать как фактор владения. МСА - интересен с точки зрения повышения степени надежности информационной безопасности. На данный момент метод представлен в виде использования вторичного канала связи для проведения цифровой аутентификации одним из выше перечисленных классических методов аутентификации. Такой подход называется внеполосным (Out-Of-Band).

Также стоит отметить частный вариант фактора владения – так называемые «magic links» (ML) - аутентификация субъекта/объекта ИС при

помощи верификации доступности ему заранее указанного некоего объекта владения.

После анализа различных систем, используемых в ИС для цифровой аутентификации субъектов/объектов ИС, были выделены некоторые критерии и свойства этих систем – результаты представлены в таблице 1.

Таблица 1

		Стоимость внедрения	Стоимость обслуживания	Степень надежности ИБ	Сложность внедрения	Производительность использования
SFA	знание	9	2	1	9	9
	владение	3	3	6	1	7
	свойство	4	8	7	5	6
2FA		4	5	8	7	6
MFA		3	3	9	2	3
OOB		4	4	8	5	7
ML		8	8	2	8	7

Оценка от 1 до 10 (где 1 – хуже, 10 – лучше)

Ввиду того, что критерии не являются взаимозаменяемыми, данный анализ не позволяет сделать выбор наилучшего метода или дать абсолютную оценку той или иной системы цифровой аутентификации, используемой в ИС, однако приведенная таблица позволяет сделать предположение о существующих запросах к системам, использующим методы цифровой аутентификации.

По итогам проведенного анализа можно сделать следующие выводы: 1) наиболее эффективными являются методы, использующие комбинацию факторов, наиболее экономически выгодными являются методы не использующие внешнее программное обеспечение или оборудование, существует высокая потребность в методах имеющих высокую производительность и высокую степень надежности; 2) недостаточность вариантов комбинирования факторов аутентификации не позволяет существующим методам значительно улучшить экономическую эффективность, повысить степень надежности с точки зрения информационной безопасности, удешевить/ускорить внедрение, разработать производительные решения для высоконагруженных ИС; 3) интересным, с точки зрения систематизации подхода к данному вопросу как предмета научного исследования, является тот факт, что все методы используют коммуникационные каналы в том или ином виде или в той или иной комбинации, и это позволяет сделать предположение о том, что, возможно, неверно использовать термин «фактор» по отношению к коммуникационным каналам. Данное предположение, а также значительный положительный тренд развития ИС, коммуникационных каналов и способов их взаимодействия и

использования позволяет нам попробовать рассмотреть МСА более углубленно.

Научный руководитель д.т.н, проф. Корченко А.Г.

Обеспечение функциональной устойчивости и кибербезопасности виртуальных облачных ресурсов систем дистанционного обучения университета

УДК 621.39:004

Б.Б.Ахметов[1],А.Б.Адранова[2]

[1]*Университет Есенова**, Актау**, Казахстан, berik.akhmetov@yu.edu.kz*

[2]*Казахский национальный педагогический университет имени Абая, Алматы, Казахстан, assel.adranova@gmail.com*

Введение. Современное развитие информационных технологий (ИТ), в учебном процессе многих крупных университетов), характеризуется широким использованием облачных ресурсов, находящихся в центрах обработки данных (ЦОД). Такие центры представляют собой совокупность серверов, располагающихся на одной площадке с целью повышения их функциональной устойчивости (ФУ) и кибернетической безопасности (КБ). В авторы так определяют облачные вычисления (ОбВ). «Это модель обеспечения повсеместного и удобного доступа посредством сети к общему пулу, включающему вычислительные ресурсы, которые подлежат настройке. К таким ресурсам можно отнести: коммуникационные сети, серверы, средства хранения данных, приложений и сервисы. Ресурсы могут быть оперативно предоставляться освобождаться с минимальными эксплуатационными затратами или обращением к провайдеру».

К облачным технологиям активно проявили интерес как крупные холдинги, которые пытаются оптимизировать свои расходы на IT-инфраструктуру предприятия, так и малые компании, или учебные заведения, которые не имеют возможности сразу развернуть свою собственную инфраструктуру. Также в качестве заинтересованных лиц выступают обычные пользователи. При этом рядовых пользователей, прежде всего, интересует возможность хранения данных, и использование программ. В ходе эксплуатации облачных ресурсов потребители заинтересованы в существенном снижении капитальных затрат на построение ЦОД, закупку серверных и сетевых компонентов оборудования, обеспечении непрерывности и работоспособности ИТ инфраструктуры своих предприятий. Все эти ресурсоёмкие и сложные вопросы при использовании облака переводятся от пользователей на провайдеров облачных услуг. Пользователь лишь оплачивает фактические услуги. Также облачные сервисы предоставляют пользователям гибкость в настройке. Например, можно самостоятельно регулировать такие параметры, как вычислительная мощность, объемы файловых хранилищ, состав программного обеспечения (ПО) и тому подобное. Несмотря на явные преимущества ОбВ возникают и проблемные вопросы. Основными из них являются следующие: недостаточное доверие к поставщику сервиса; необходимость надежно обеспечить конфиденциальность, целостность,