МОДЕЛЬ ПРЕДСТАВЛЕНИЯ ДАННЫХ И ИДЕНТИФИКАЦИИ В СЕРВИСНЫХ ПОДСЕТЯХ. ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИИ СИСТЕМ ЕДИНОГО ВХОДА

Зеленцова Ж.Ю.[1], Йона Е.О.[2], Волков С.Л.[3], к.т.н., доцент.
1 – ТОВ «Network Cloud Cube-2», м. Кременчук,
2 – Одесский национальный экономический университет,
3 - Одесская государственная академия технического регулирования и качества, г. Одеса

Глобальная вычислительная среда становится все более разнообразной по количеству предоставляемых сервисов. В результате возникает необходимость их интеграции в рамках единой пользовательской платформы, подразумевающей поддержку единого входа. В рамках этой проблемы нужно рассматривать архитектурные особенности интеграционных систем, т.к. существует ряд ограничений и требований безопасности, которые должны быть учтены при разработке сервисов идентификации. Также интенсивно развивается сетевая инфраструктура, что подразумевает изменение и архитектурных принципов.

Целью доклада является обоснование систем идентификации и обеспечения доступа с единым входом (англ.: *Single Sign-On* [SSO]), адаптированных к текущим особенностям сервисных систем. Такие системы предложены целым рядом производителей и готовятся к повсеместному использованию.

Результаты исследования. Технология единого входа SSO – одна из технологий, относящихся к широкому классу систем управления идентификацией и доступом пользователей (англ.: *Identity management and access* [IAM]). Основное отличие технологии SSO состоит в совмещении процессов идентификации (ID) и аутентификации (AuthN) с единой точкой отказа. Эту технологию на сегодняшний день реализует ряд производителей VMware, Google, Pay Pal. Ими отмечается ряд проблемных вопросов и уязвимостей архитектурного уровня, которые непременно будут оказывать значительное влияние на процесс развития систем при текущих признаках цифровой вселенной (англ.: *Digital Universe*) – при росте количества пользователей, устройств, данных, а также при расширении сервисных возможностей сети.

Предлагаемая здесь к анализу тема рассматривалась в рамках задачи организации единого входа в сервисной подсети. Как подчеркивается в [1-3], для современной сетевой инфраструктуры свойственно большое количество пользователей, устройств и данных. Стремительно растет количество низкопроизводительных устройств типа Internet of Things (IoT) или «интернет-вещей». По версии IDC, количество уникальных подключений в 2020 году достигнет 212 млрд. Наращивание количества подключений будет происходить в четырех сервисных сегментах: *мобильных технологий*, *медиа*, «*облачных» сервисов* и *средств безопасности*. Также в своем отчете компания Akamai, подчеркивает необходимость разработки hyper-connected платформ, ориентированных на обслуживание большого количества уникальных подключений, которое будет характерно для сервисных платформ в среднесрочной перспективе.

Относительно сегментации пользователей, эксперты отмечают последующую сегментацию сервисных сетей, что подразумевает формирование различий в восприятии потребителей между государственными, «облачными» и частными внедрениями. Т. о., исследование процесса развития направления сервисных подсетей, агрегирующих определенное количество сервисов, работающих с большим количеством пользователей посредством устройств и генерирующих данные, является актуальным и востребованным.

Архитектурные особенности мультисервисной платформы, о которой ведется речь, отмечены на рис. 1.

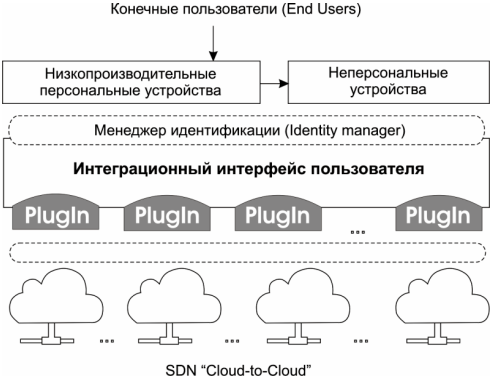

Рисунок 1 - Архитектура сервисной подсети «облачного» типа

Как следует из рис. 1 и показано в [1-3], платформа имеет сервис-ориентированную архитектуру (англ.: *Service-Oriented Architecture* [SOA]). Она представляет собой набор высокопроизводительных и низкопроизводительных ресурсов, объединенных между собой посредством слоя виртуализации разных интеграционных уровней. Зона высокопроизводительных ресурсов объединена с зоной низкопроизводительных ресурсов (устройствами пользователей) с помощью слоя сопряжения – «облачного» слоя. Каждое облако является отдельным сервисом или представляет собой платформу сервисов PaaS. Сервисы между собой взаимно-интегрированы с помощью технологии программно-конфигурируемых сетей (англ.: *Software-defined Networking* [SDN]) с топологией «cloud-to-cloud». Подсеть предусматривает интеграцию сервисов-«облаков» в один интерфейс, которые могут быть слабосвязными. При этом обеспечивается «бесшовное» подключение сервисов различных поставщиков решений. Сервисы-«облака» предоставляют услуги конечному пользователю посредством интеграционного интерфейса пользователя и подключаются по типу Plug-In. Для подключения большого количества сервисов запросы унифицированы по принципу SLA-запросов (англ.: *Service Level Agreement* [SLA]).

Интеграционная сервисная платформа с приведенной архитектурой может управлять идентификацией и доступом с помощью менеджера идентификации (англ.: *Identity Manager*), основанного на технологии единого входа SSO и обеспечивающего идентификацию пользователя в различных сервисных

составляющих, подключенных к подсети (рис. 1). Решение, касающееся менеджера идентичностей, использовано из Dell One Identity.

В совокупности системы управления идентификацией (англ.: *Identity-Management Systems*) управляют процессом цифровой идентификации устройств посредством выявления данных о пользователях с помощью аппаратных и программных методов. Сам процесс идентификации может значительно отличаться в зависимости от архитектурных особенностей сетевых сред, а проектирование систем доступа должно учитывать архитектурные особенности и технологические тренды, предполагающие изменения процесса доступа к сервисным платформам.

Процесс управления учетными записями и доступом IAM классически состоит из нескольких подпроцессов:

– *управления идентификацией и учетными записями* (англ.: *Identity Management* [IdM]), состоящего из управления жизненным циклом идентичностей и администрирования учетных записей;

– *управления доступом* (англ.: *Access Management* [AM]), состоящего из аутентификации [AuthN] и авторизации [AuthZ];

– *контроллинга, управления рисками и соответствия требованиям* (англ.: *Governance, Risk and Compliance* [GRC]), состоящего из сбора информации для аудита, отчета о действиях (Actionable reports), оценки и контроля рисков (Risk Management), соответствия государственным и корпоративным стандартам (Compliance).

Существует целый ряд технологий, которые могут быть использованы как составляющие систем IAM. Так, это: системы контроля доступа (англ.: *Access Control*); цифровые удостоверения (англ.: *Digital Identities*); менеджеры паролей (англ.: *Password Managers*), агрегирующие пароли разных систем и обеспечивающие «быстрый» доступ с идентифицированных устройств; системы единого входа (англ.: *Single Sign-on*); маркеры безопасности (англ.: *Security Tokens*), система глобальной идентификации OpenID.

Идентификация в теоретических и практических моделях строится на получении некоторой модели с набором идентифицирующих атрибутов [10]. К идеальным моделям относят модель «чистой идентичности» (англ.: *Pure Identity*). На практике обычно рассматривают только некоторые аспекты идентичности в рамках построенной агрегирующей семантической модели – такой подход не подразумевает совпадение полного набора параметров.

Семантическая модель, в свою очередь, состоит из внешних и внутренних паттернов. Модель «чистой идентичности» связана только внутренними паттернами, т. е. не зависит от работы приложения в котором проходит идентификация и других факторов. На практике применяются несколько моделей определения идентичности, обеспечивая разброс параметров. В результате снижается погрешность распознавания при выполнении условий упрощения доступа. Модели демонстрируются в процессе доклада. В итоге делается вывод о том, что предложен подход, который позволяет создать защищенные государственные депозитарии связных официальных и неофициальных данных о сетевых пользователях, а также избавиться от необходимости особого режима обработки персональных данных для каждой отдельной организации, на сегодняшний день нормированного законодательно.

Література

1. Зеленцова Ж. Ю. Конвергенция глобальной сети как новый этап развития: обзор инфраструктурных решений и технологий с целью нахождения решений для повышения безопасности обработки данных при облачных вычислениях [Текст] / Ж. Ю. Зеленцова, Н. Ф. Казакова // Інформаційна безпека. – 2013. – № 4 (12). – С. 23-40.
2. Зеленцова Ж. Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях [Текст] / Ж. Зеленцова, Н. Казакова // Захист інформації і безпека інформаційних систем : III міжнар. наук.-техн. конф., 5-6 червня 2014 р. : матер. конф. – Львів, НУ «Львівська політехніка. – С. 58-59.
3. Казакова Н. Ф. Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Системи обробки інформації. – 2014. – Т. 2, № 2(118). – С. 246.
4. Луговой А. В. Эра - мегаданных. Состояние и эволюция мирового информационно-вычислительного пространства [Текст] / А. В. Луговой, Ж. Ю. Зеленцова, О. В. Луговая // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2012. –Т. 1, № 1/2012 (72). – С. 36-42.
5. Казакова Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки / Н. Ф. Казакова, Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – Т. 1, № 15(204). – С. 172-181.
6. Зеленцова Ж. Ю. Уязвимости конвергентной инфраструктуры и практические подходы к их устранению [Текст] / Ж. Ю. Зеленцова, А. В. Луговой // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – Т. 1. – № 15(204). – С. 122-129.
7. Зеленцова Ж. Ю. Анализ архитектуры глобальны х конвергентных решений и синтез агрегированной модели [Текст] / Ж. Ю. Зеленцова, А. В. Луговой // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2013. – № 3. – С. 80.
8. Луговой А. В. Эра мегаданных. Состояние и эволюция мирового информационно-вычислительного пространства [Текст] / А. В. Луговой, Ж. Ю. Зеленцова, О. В. Луговая // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2012. – С. 36-42.
9. Зеленцова Ж. Ю. Унифицированная технологическая модель конвергентной инфраструктуры [Текст] / Ж. Ю. Зеленцова // Комп'ютерні системи та мережні технології : VI Міжнар. наук.-техн. конф. CSNT-2013, 11-13 червня 2013 р. : збірн. тез. – Київ, НАУ. – С. 81.
10. Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. О. Йона, Є. В. Вавілов, К. Б. Айвазова // ОНЕУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.