DOI 10.37882/2223–2966.2021.01.04

АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА В ОБЛАЧНЫХ СИСТЕМАХ

ANALYSIS OF THE POSSIBILITY OF USING BIOMETRIC AUTHENTICATION FOR ACCESS CONTROL IN CLOUD SYSTEMS

A. Barsolevskaya
D. Kondrashkin
V. Samoylov
S. Volkov

Summary. The article touches upon the problems of information security of remote working employees operating in companies with a cloud-based infrastructure. The degree of influence of the authentication system on the reliability of the information security system is analyzed based on the CVSS (common vulnerability scoring system). A comparative analysis of the reliability of two-factor biometric and password authentication systems is carried out by assessing the probabilities of successful attacks. Furthermore, a two-factor biometric authentication scheme is proposed for working with cloud-based structures.

Keywords: authentication system, access control, biometric characteristics, two-factor authentication, type II error.

Барзолевская Анна Федоровна
ФГБОУ ВО «Московский Государственный Лингвистический Университет», Москва
a.barzolevskaia@gmail.com
Кондрашкин Дмитрий Александрович
ФГБОУ ВО «Московский Государственный Лингвистический Университет», Москва
jakekondr@gmail.com
Самойлов Вячеслав Евгеньевич
К.т.н., ФГБОУ ВО «Московский Государственный Лингвистический Университет», Москва
v.samoilov@linguanet.ru
Волков Сергей Дмитриевич
Аспирант, ФГБОУ ВО «Московский Государственный Лингвистический Университет», Москва
volkov1234@gmail.com

Аннотация. В статье рассматриваются проблемы информационной безопасности удаленной работы сотрудников с облачными структурами компаний. На основании системы общего учета уязвимостей CVSS анализируется степень влияния системы аутентификации на надёжность системы защиты информации, проводится сравнительный анализ надёжности двухфакторных систем биометрической и парольной аутентификации, посредством оценки вероятности «удачной» атаки. А также, предлагается схема двухфакторной биометрической аутентификации для работы с облачными структурами.

Ключевые слова: система аутентификации, разграничение доступа, биометрические характеристики, двухфакторная аутентификация, ошибка второго рода.

Введение

Процесс цифровизации российской экономики постепенно захватывает новые области и приобретает новые формы. Одной из таких форм является дистанционная (удаленная) работа — это особая форма организации трудового процесса, при которой сотрудники компании выполняют свои трудовые функции вне рабочего пространства, а их коммуникация в процессе работы осуществляется посредством цифровых технологий. Сравнительно недавно такая трудовая форма была скорее исключением, чем обыденностью, однако эпидемия вируса COVID-19 внесла свои коррективы в процессы развития человеческого общества. Безусловно, удаленная работа возможна далеко не во всех видах деятельности, но обстоятельства заставляют человека приспосабливаться и видоизменять традиционные способы взаимодействия.

После появления вируса COVID-19 на территории Российской Федерации Указ Президента РФ от 25.03.2020 N206 «Об объявлении в Российской Федерации нерабочих дней» [1] положил начало серии правовых актов, которые вводили меры по обеспечению санитарно-эпидемиологического благополучия населения на территории нашей страны. Федеральное и региональное Правительство на волне противоэпидемических и профилактических мероприятий обратилось к работодателям с рекомендацией по принятию вспомогательных мер, в том числе использованию гибких форм занятости, а именно удаленной, дистанционной и надомной работы. А в конце 2020 года был подготовлен и принят Феде-

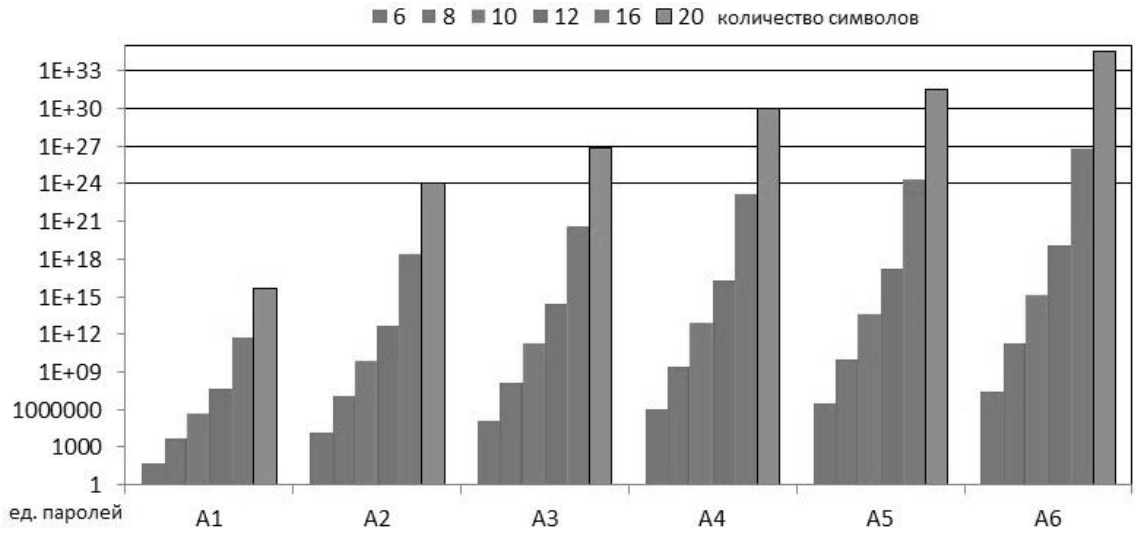

Рис. 1. Зависимость среднего времени подбора пароля от используемого алфавита и длины пароля

ральный закон от 8 декабря 2020 г. N407-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях» [2]. Закон вступил в силу с 1 января 2021 года.

Закон вводит три ключевых понятия: дистанционная (удаленная) работа; временная дистанционная (удаленная) работа — режим, предусматривающий временное выполнение трудовой функции вне стационарного рабочего места, находящегося под контролем работодателя; комбинированная дистанционная (удаленная) работа — стационарная занятость на рабочем месте и дистанционная (удаленная) работа.

Развитие указанных в [2] форм работы способствует повышенному интересу компаний к созданию собственных или использованию существующих облачных структур. Явные преимущества в виде снижения объёмов арендной платы и снижения хозяйственных расходов на содержание офисов предопределяют заинтересованность коммерческих организаций в переводе сотрудников на удалённую работу. Однако, отсутствие системного контроля за действиями сотрудников, находящихся вне территории работодателя, в очередной раз делает актуальным вопрос об информационной безопасности использования информационных систем (ИС), функционирующих на основе технологии облачных вычислений.

Постановка задачи

Ключевой частью ИС, построенной на технологии облачных вычислений, является система аутентификации, она реализует функцию защиты информации и осуществляет разделение доступа пользователей. Большинство протоколов аутентификации используемых в облачных структурах используют однофакторную или многофакторную парольную защиту [3–5]. Современные алгоритмы поиска и перебора паролей достигают своих целей за сравнительно небольшие сроки. На рисунке 1 приведены зависимости среднего времени подбора пароля от используемого алфавита и длины пароля [6].

Очевидно, что решением данной проблемы является усложнение требований к паролю, согласно [6] он должен составлять не менее 8–12 символов и состоять из алфавитов A5 и A6. Однако, постоянное усложнение паролей приводит к появлению уязвимостей другого рода — повышается вероятность утери пароля пользователем. Пользователи склонны к записи и сохранению сложных паролей. Кроме того, бесчисленный рост систем, требующих персональной аутентификации, увеличивает число пар «логин-пароль», которые необходимо запомнить и постоянно использовать (проблема «многих входов»), что также приносит определённые риски со стороны пользователей.

Для решения проблемы «многих входов» часто используют схему однократного входа с авторизацией SSO (Single Sign-On). Управление доступом по схеме SSO даёт возможность пользователям корпоративной сети при их входе в сеть пройти только одну аутентификацию, предъявив только один раз пароль, и затем без дополнительной аутентификации получить доступ ко всем авторизованным сетевым ресурсам, которые нужны для выполнения их работы [5]. Использование данной схемы повышает производительность труда пользователей, повышает информационную безопасность систем, сни-

Таблица 1. Показатели аутентификации

Показатель	Описание показателя	Вес
Многоразовая аутентификация	Эксплуатация уязвимости требует, чтобы пользователь провел аутентификацию несколько раз. Например, пользователю необходимо осуществить вход в ОС, а затем в бизнес-приложение	0,450
Одноразовая аутентификация	Эксплуатация уязвимости требует прохождения аутентификации один раз	0,560
Аутентификация отсутствует	Эксплуатация уязвимости не требует аутентификации	0,704

Таблица 2. Изменение значений базовой метрики CVSS для разных систем аутентификации

Показатель	Вектор CVSS	Значение
Многоразовая аутентификация	AV: A/AC: M/Au: M/C: P/I: P/A: P	4,5
Одноразовая аутентификация	AV: A/AC: M/Au: S/C: P/I: P/A: P	4,9
Аутентификация отсутствует	AV: A/AC: M/Au: N/C: P/I: P/A: P	5,4

жая вероятность утери паролей пользователем, однако не решает проблемы развития алгоритмов подбора паролей.

Очевидным решением данной задачи является использование биометрических характеристик человека для доступа к ресурсам облачных структур компаний. Современные ноутбуки и смартфоны обеспечены высококачественными видеокамерами и звуковыми картами, что привело к масштабному распространению и развитию технологий Face ID и Voice ID.

Количественная оценка риска подбора пароля в системе аутентификации ИС, построенной на технологии облачных вычислений

Для проведения количественной оценки и построения риск-модели облачной среды используются базовые векторы системы общего учета уязвимостей (CVSS) [7, 8]. В данной системе особое место отводится процессу аутентификации, он описывает количество необходимых сеансов аутентификации цели при эксплуатации уязвимости. Показатель не учитывает сложности данного процесса, а лишь характеризует саму необходимость аутентификации для использования уязвимости [7].

Расчет базовой метрики производится по следующей формуле:

$$BS = round\_to\_1\_decimal\{[(0{,}6imp) + \\ + (0{,}4Exp) - 1{,}5] + f(imp)\},$$

где BS — базовая метрика;
imp — общее влияние (урон), определяемое как

$$imp = 10{,}41[1 - (1 - Confimp)(1 - \\ - Intimp)(1 - Avimp)],$$

где $Confimp$ — урон конфиденциальности;
$Intimp$ — урон целостности;
$Avimp$ — урон доступности;
Exp — доступность использования эксплойта, определяемая как

$$Exp = 20AccVec \cdot AccCom \cdot Aut,$$

где $AccVec$ — вектор доступа,
$AccCom$ — вектор сложности;
Aut — аутентификация;
$f(imp) = 0$, если $imp = 0$, в других случаях $f = 1{,}176$.

Показатели аутентификации определяются коэффициентами, представленными в таблице 1. Очевидно, что с усложнением системы аутентификации изменяется и количественная оценка рисков для облачной системы, но в таблице 1 не приведено значение весового коэффициента для биометрической аутентификации. Возникает вопрос, является ли эта технология более надёжной с точки зрения информационной безопасности?

Рассмотрим изменение количественной оценки рисков облачной системы для заданных параметров при условии, что система аутентификации меняется. Результаты моделирования представлены в таблице 2.

Результаты анализа изменения значений базовой метрики CVSS позволяют сделать вывод о том, что для «неидеальной» с точки зрения информационной безопасности системы усложнение схемы аутентификации существенно влияет на её защиту.

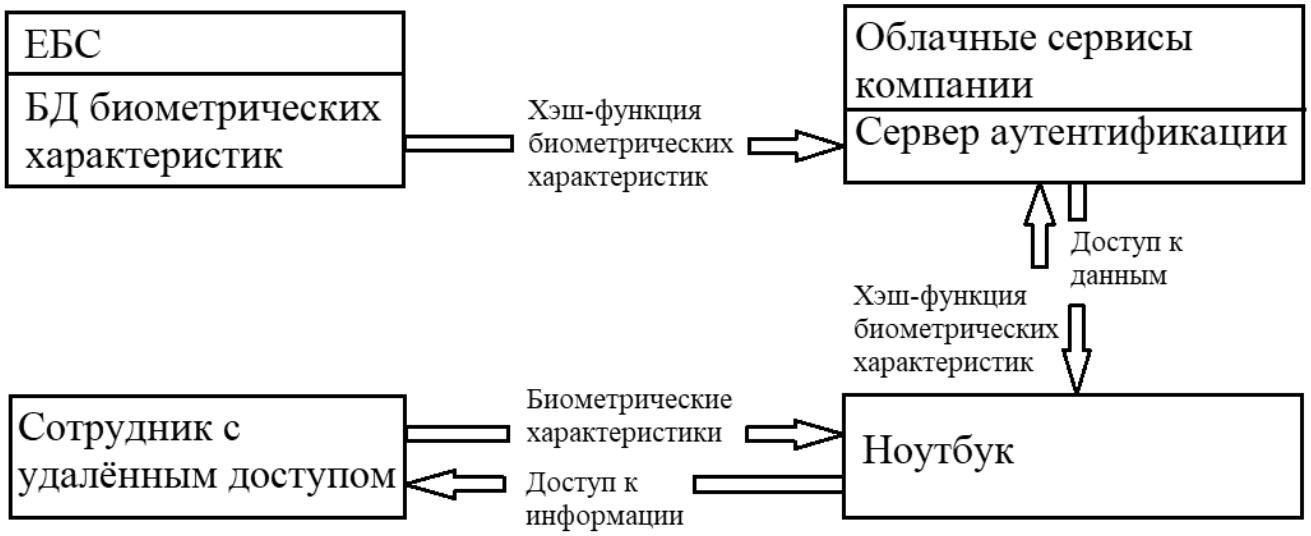

Рис. 2. Схема двухфакторной биометрической аутентификации при работе с облачными структурами

Оценка вероятности «удачной» атаки на систему биометрической и парольной аутентификации

Для сравнительного анализа надёжности систем биометрической и парольной аутентификации необходимо определить вероятности «удачной» атаки. Для качественного анализа необходимо сравнивать двухфакторную аутентификацию, как наиболее распространённую и в должной мере надёжную.

Вероятность «удачной» атаки на двухфакторную систему парольной аутентификации определяется формулой

$$p_{\text{п}} = p_{1\text{п}}p_{2\text{п}} + p_{2\text{рп}},$$

где $p_{1\text{п}}$ — вероятность подбора первого пароля за приемлемое время;

$p_{2\text{п}}$ — вероятность подбора второго пароля за приемлемое время;

$p_{2\text{рп}}$ — вероятность ошибки второго рода двухфакторной системы парольной аутентификации.

Очевидно, что $p_{2\text{рп}} \ll 0$, поэтому результирующая формула для оценки вероятности «удачной» атаки на двухфакторную систему парольной аутентификации будет

$$p_{\text{п}} = p_{1\text{п}}p_{2\text{п}}.$$

По аналогии вероятность «удачной» атаки на двухфакторную систему биометрической аутентификации определяется формулой

$$p_{\text{б}} = p_{1\text{г}}p_{2\text{л}} + p_{2\text{рб}},$$

где $p_{1\text{г}}$ — вероятность подбора голосового пароля;

$p_{2\text{л}}$ — вероятность подбора геометрии лица;

$p_{2\text{рб}}$ — вероятность ошибки второго рода двухфакторной системы биометрической аутентификации.

Известно, что для систем биометрической аутентификации вероятность второго рода $p_{2\text{рп}} \neq 0$. Для голосовой аутентификации вероятность ошибок второго рода велика, порядка 10^{-2}, для систем аутентификации на основе геометрии лица этот параметр значительно меньше, и составляет 10^{-6} [9, 10].

Результирующее значение вероятность ошибки второго рода для комбинации систем аутентификации по голосу и по геометрии лица составит

$$p_{2\text{рб}} = p_{2\text{рг}}p_{2\text{рл}} = 10^{-2} \cdot 10^{-6} = 10^{-8}.$$

Учитывая, что задача подбора образцов голоса и формы лица гораздо более сложна, чем задача подбора пароля, можно сделать вывод о повышении безопасности ИС при использовании комбинированной двухфакторной биометрической аутентификации.

Применение двухфакторной биометрической аутентификации в облачных структурах

С 2019 года в Российской Федерации ведётся сбор биометрических данных граждан в Единую биометрическую систему (ЕБС). ЕБС работает совместно с Единой системой идентификации и аутентификации (ЕСИА), эти системы

позволяют проводить идентификацию и аутентификацию человека с вероятностью 99,99% (ошибка второго рода лежит в допустимых пределах и составляет $10^{-6} \div 10^{-8}$). В ЕБС используются одновременно два параметра — голос и лицо, что позволяет однозначно определить человека, а не его имитацию. Биометрическая информация в ЕБС хранится в виде односторонней хэш-функции.

В рамках актуальности задачи повышения безопасности использования облачных сервисов для осуществления удалённой работы сотрудников компаний, предлагается использовать биометрическую аутентификацию для доступа сотрудников к облачным ресурсам. Схема аутентификации представлена на рисунке 2.

Анализ предложенного подхода выявляет решение нескольких очевидных проблем:

1. После увольнения сотрудника из компании нет необходимости удалять его профили и пароли. Паролем уволенного сотрудника никто не сможет воспользоваться.
2. Отсутствие необходимости использования SSO систем. Все системы, требующие аутентификации, заводятся на надёжную биометрическую защиту.
3. Пользователь не может потерять или передать кому-либо свой пароль.

Заключение

В работе были рассмотрены проблемы информационной безопасности удаленной работы сотрудников с облачными структурами компаний. Определена актуальность задачи повышения сложности систем аутентификации для ИС, построенных на технологии облачных вычислений. Проведён анализ степени влияния системы аутентификации на надёжность системы защиты информации. Результаты анализа изменения значений базовой метрики CVSS казали, что усложнение схемы аутентификации существенно влияет на защиту ИС.

Проведен сравнительный анализ надёжности двухфакторных систем биометрической и парольной аутентификации, посредством оценки вероятности «удачной» атаки. В результате чего было определено, что при использовании комбинированной двухфакторной биометрической аутентификации безопасность ИС повышается.

А также, была предложена схема двухфакторной биометрической аутентификации при работе с облачными структурами, которая позволяет снизить влияние нескольких уязвимостей, связанных с особенностями работы пользователей.

ЛИТЕРАТУРА

1. Указ Президента РФ от 25.03.2020 N206 «Об объявлении в Российской Федерации нерабочих дней»// «Собрание законодательства РФ», 30.03.2020, N13, ст. 1898 // Официальный сайт Президента России — http://www.kremlin.ru/acts/bank/45335–2020. — 25 марта.
2. Федеральный закон от 8 декабря 2020 г. N407-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях» // Информационно-правовой портал Гарант.ру — https://www.garant.ru/products/ipo/prime/doc/74915881/ — 2021. — 8 декабря.
3. Минакова Н.Н., Поляков В. В., Толстошеев С. Н. Методы технической и правовой защиты информации в сети Интернет.— Барнаул: Алтайский государственный университет, 2015. — 155 с.
4. Роганов В. А., Кузнецов А. А., Матвеев Г. А., Осипов В. И. Адаптивный анализ надежности паролей при помощи гибридных суперЭВМ // Программные системы: теория и приложения. 2015. Т. 6. № 4 (27). С. 139–155.
5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей «Информатика и вычислительная техника».— Москва: Форум: ИНФРА-М, 2012. — 415 с.
6. Блинов А. С., Степаненко М. А. Оценка достаточной сложности пароля для безопасного использования на веб-ресурсах // Исследования в области естественных наук. 2014. № 8 (32). С. 24–27.
7. Блохина О. В., Логинова А. О., Царегородцев А. В. Методика количественной оценки риска информационной безопасности для облачной инфраструктуры организации // Огарёв-Online. 2018. № 14 (119). С. 3.
8. Царегородцев А. В., Макаренко Е. В. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Дайджест-финансы. 2015. № 1 (233). С. 56–67.
9. Газин А. И. Особенности голосовой аутентификации личности // Труды международного симпозиума «Надежность и качество». 2010. Т. 2. С. 232–235.
10. Иванова А. В., Михайлова У. В., Баранкова И. И. Уязвимости биометрической защиты // Актуальные проблемы современной науки, техники и образования. 2020. Т. 11. № 1. С. 68–72.

© Барзолевская Анна Федоровна (a.barzolevskaia@gmail.com), Кондрашкин Дмитрий Александрович (jakekondr@gmail.com), Самойлов Вячеслав Евгеньевич (v.samoilov@linguanet.ru), Волков Сергей Дмитриевич (volkov1234@gmail.com).
Журнал «Современная наука: актуальные проблемы теории и практики»