УДК 004.056.52
DOI: 10.33764/2618-981X-2021-8-314-323

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДОСТОИНСТВ И НЕДОСТАТКОВ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ МЕТОДОВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ И ДРУГИХ УЧАСТНИКОВ ИДЕНТИФИКАЦИОННЫХ ПРОЦЕССОВ

Сергей Васильевич Десятов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. +7 (913) 785-86-85, e-mail: s.v.desyatov@sgugit.ru

В статье подробно рассмотрены как достоинства, так и недостатки наиболее часто применяемых методов идентификации и аутентификации. Приведена сравнительная характеристика различных типов персональных идентификаторов. Обращено внимание на необходимость комплексного подхода к решению задач идентификации и аутентификации.

Ключевые слова: информационные технологии, информационная безопасность, идентификация, аутентификация, пароль, токен, информационное пространство

COMPARATIVE ANALYSIS OF ADVANTAGES AND DISADVANTAGES OF THE MOST COMMON METHODS OF IDENTIFICATION AND AUTHENTICATION OF USERS AND OTHER PARTICIPANTS OF IDENTIFICATION PROCESSES

Sergey V. Desyatov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: +7 (913) 785-86-85, e-mail: s.v.desyatov@sgugit.ru

The article discusses in detail both the advantages and disadvantages of the most commonly used identification and authentication methods. Comparative characteristics of different types of personal identifiers are carried out. Attention is drawn to the need for an integrated approach to solving problems of identification and authentication.

Keywords: information technologies, information security, identification, authentication, password, token, information space

Введение

Если внимательно взглянуть на схему развития человечества, так называемые технологические уклады, предложенную русским экономистом Кондратьевым, то мы оказываемся в пятом из шести укладов. Причем это завершение фазы роста и переход в фазу зрелости.

Согласно определению, технологический уклад – это совокупность сопряженных производств, имеющих единый технический уровень и развивающихся синхронно. Смену доминирующих в экономике технологических укладов предопределяет не только ход научно-технического прогресса, но и инерция мышления общества, новые технологии появляются значительно раньше их массового освоения.

Основными отраслями пятого технологического уклада являются: электроника и микроэлектроника, информационные технологии, генная инженерия, программное обеспечение телекоммуникации, освоение космического пространства. К гуманитарным преимуществам этого уклада относятся глобализация, скорость связи и перемещения.

Информационные технологии являются неотъемлемой частью нашей жизни. Они оказывают и будут оказывать существенное влияние на все сферы экономики. Эксперты в один голос говорят о приближении эры «цифровой» трансформации. Рост объема обрабатываемых данных и цифровизация дают субъектам экономики новые преимущества, но в то же время приводят к повелению дополнительных рисков. Поэтому сегодня так важно оперативно реагировать на новые угрозы и предпринимать ответные действия на всевозможные кибератаки, пока ущерб от них не поставил под угрозу не только конкретные предприятия, отрасль экономики, но и всю экономику в целом.

Нет большой необходимости постоянно подчеркивать важность информационной безопасности. Достаточно просто посмотреть статистику средней стоимости ущерба от инцидентов информационной безопасности не только в России, но и в других странах мира. Есть полное понимание у всех специалистов, работающих как в области IT-технологий, так в области информационной безопасности: ущерб от киберпреступности в мировой экономике ежегодно оценивается в сумму более 1 трлн долларов, а рынок информационной безопасности также растет очень высокими темпами и по самым скромным подсчетам перевалит в этом году за 200–250 млрд. долларов.

Приведенные выше цифры условны, но важна тенденция – растет ущерб и, соответственно, растут расходы на предотвращение возможных неблагоприятных последствий.

Следует отметить еще одну немаловажную тенденцию: от утечек данных, как персональных, так и корпоративных, в настоящее время во всем мире пострадало, как минимум, 1,5–2 миллиарда людей, что требует ужесточения регулирования и развития альтернативных методов аутентификации. К ним, в первую очередь, относится авторизация с помощью биометрии: в прошлом (2020) году с ее помощью осуществлялось четверть всех мировых электронных транзакций.

Хочется привести одну старую аксиому: «Все новое – это хорошо забытое старое». Исходя из сложившихся обстоятельств, иногда проще, эффективнее и надежнее воспользоваться уже имеющимся набором инструментов, чему есть масса примеров из нашей жизни, техники и производства.

Взаимодействие всех типов идентификационной информации

Прежде чем тщательно рассматривать заявленную тему, необходимо вспомнить базовые определения вышеназванных средств защиты:

– аутентификация – это процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является тем, за кого себя выдает;

– идентификация – это тоже процесс, в ходе которого выполняются права доступа, привилегии, свойства и характеристики пользователя на основе его имени, логина или какой-либо другой информации о нем.

Несомненно, идентификация и аутентификация являются ключевым элементом при использовании современных программно-технических методов защиты информационной среды. Прежде чем говорить о достоверности участника информационного взаимодействия, его необходимо идентифицировать. И здесь важнейшая задача заключается в определении «кто есть кто»: из имеющегося списка всех участников, зарегистрированных в информационной системе, на базе уникального идентификатора (имени субъекта), выбирается пользователь, отвечающий заданным параметрам обеспечения безопасности. Если процедура ввода идентификатора прошла успешно, то следующим шагом в системе обеспечения безопасности является процесс аутентификации (подтверждение пользователя тем, за кого он себя выдает).

Как показывает практика, аутентификационную информацию (по которой идентифицируется пользователь), можно подразделить на три типа:

– субъект обладает уникальной конфиденциальной или секретной информацией (например, пароль);

– субъект обладает каким-либо предметом с уникальной информацией (например, USB-ключ);

– субъект обладает информацией, которая является неотъемлемой его частью: биометрическая аутентификация (отпечатки пальцев, радужная оболочка глаза, голос, образец рукописной подписи и т.д.)

Идентификация и аутентификация являются взаимосвязанными и взаимодополняющими процессами распознавания и проверки подлинности пользователя информационных сетей. Именно от них зависит дальнейшее решение системы – можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После успешного завершения процессов идентификации и аутентификации субъекта выполняется его авторизация (вход в систему).

Имеющиеся в настоящее время механизмы обеспечения безопасности информационного пространства имеют в своем распоряжении достаточно надежные и эффективные средства защиты, которые обладают как преимуществами, так и недостатками. Они могут использоваться в различных комбинациях и в совокупности с выбором определенных методов и инструментов системы безопасности [1].

Достоинства и недостатки идентификации и аутентификации

Итак, начнем рассмотрение достоинств и недостатков наиболее распространенных методов идентификации и аутентификации.

1. Пароль.

К очевидным достоинствам можно отнести то, что он – «первопроходец», т.к. появился намного раньше остальных, и в настоящее время используется по-

всеместно, в огромном количестве. Кроме того, возможна двухфакторная аутентификация с использованием одноразовых паролей.

Явные недостатки обусловлены тем, что пользователи выбирают простые или легко угадываемые пароли. Пароль могут подсмотреть или перехватить при вводе. Пароль пользователя могут получить обманным путем. Не исключены ситуации, когда пароль может быть похищен или отнят у его владельца.

2. Уникальный предмет: смарт-карта, карта с магнитной полоской, USB-ключи.

Достоинства данных предметов заключается в том, что они уникальны, благодаря содержащихся в них информации. Простота использования: содержащаяся на носителе информация (пароль и идентификатор пользователя) легко считывается с него и транслируется на модуль аутентификации. Уникальный предмет может использоваться в качестве одного из элементов аутентификации двухфакторным методом.

К недостаткам данного метода следует отнести то, что в большинстве случаев требуется специальное оборудование для работы с предметами. Не исключена возможность изготовления копии или эмулятора предмета. Как и в случае с паролем, предмет может быть похищен или отнят у его владельца.

3. Биометрические средства.

Достоинства в их исключительной индивидуальности для каждого пользователя. Их обычно подразделяют на:

– статические (физиологические): отпечатки пальцев, черты лица, характеристики оболочки глаза и др.;

– динамические (поведенческие): голос, образец рукописной подписи, «клавиатурный почерк» (интервал времени между нажатиями клавиш, составляющих кодовое слово, интенсивность нажатий) и др.;

– комбинированные (статические и динамические) [8].

На первый взгляд может показаться странным, но основной недостаток биометрических характеристик заключается в том, что они являются уникальными идентификаторами. Биометрические идентификаторы обеспечивают очень высокие показатели эффективности. Вероятность несанкционированного доступа лежит в пределах от 0,1 до 0,0001%!

Не исключена возможность двухфакторной аутентификации – к устройству сканирования могут элементарно поднести муляж.

Биометрические данные человека не являются чем-то постоянным. Отдельные биометрические данные меняются как в результате старения, так и травм, ожогов, порезов, различных болезней и т.д.

Если у Вас украдут биометрические данные или их компрометируют, то это, как правило, на всю жизнь. Биометрические характеристики нельзя сохранить в секрете.

Как было рассмотрено выше, каждому методу идентификации и аутентификации присущи определенные достоинства и недостатки, но важно понимать, что многое зависит и от требований, предъявленных к конкретному процессу защиты данных. Необходимое условие – соблюдение пользователем повышенных

мер безопасности. С целью достижения более высокого уровня безопасности информационного пространства имеющиеся средства аутентификации могут использоваться, как по отдельности, так и в комплексном (комбинированном) виде.

Следует иметь в виду, что в сетевой среде, в случае, если стороны идентификации и аутентификации территориально разделены, то у такого процесса можно выделить два важных аспекта системы безопасности:

– что служит аутентификатором,

– насколько эффективно защищен обмен данными идентификации и аутентификации.

В настоящее время методический аппарат анализа рисков информационной безопасности, проектирования и сопровождения систем безопасности позволяет с высокой степенью вероятности оценить текущий уровень безопасности с учетом потенциальных рисков в информационной среде.

Несовершенство применяемых стандартных «многоразовых» паролей и, как следствие, высокий уровень уязвимости в системе безопасности в процессе работы на постороннем оборудовании, послужили толчком к развитию рынка аутентификации и созданию аппаратных генераторов «одноразовых паролей».

В основе такой методики с использованием многофакторной аутентификации заложено применение персональных аппаратных устройств – токенов, которые поддерживают несколько методов аутентификации и представляют собой своего рода электронный ключ для доступа к информационным активам. Это может быть электронная подпись, биометрические данные, криптографический ключ. Токены довольно универсальны: они могут использоваться как вместо пароля, как и вместе с ним, кроме того, позволяют генерировать и хранить ключи шифрования, обеспечивая тем самым строгую аутентификацию.

Попробуем рассмотреть несколько видов токенов с точки зрения как преимуществ, так и недостатков.

1. USB-токены. В числе преимуществ – мобильность (токен можно использовать на любом компьютере, где есть USB-порт). Возможность поддержки большого числа приложений IT-безопасности. Очевидная принадлежность токена пользователю.

К числу недостатков следует отнести необходимость установки ПО пользователю.

2. Смарт-карты. Несомненным преимуществом этого типа токенов (идентификаторов) являются высокий уровень безопасности, небольшие габариты, поддержка большого числа применений и очевидная принадлежность пользователю.

К недостаткам следует отнести требование установки ПО пользователю и низкая мобильность (требуется считывающее устройство). Следует заметить, что в данном случае преимущества преобладают над недостатками.

3. USB-токены со встроенным чипом. Преимущества: высокий уровень безопасности, мобильность, поддержка большого числа приложений и очевидная принадлежность пользователю. На серьезном фоне преимуществ один небольшой недостаток, характерный для всех вышерассмотренных типов токенов – требуется установка ПО пользователю.

4. Программные токены. Данному типу токенов не требуются аппаратное устройство. Однако количество недостатков возрастает. В их числе слабая защищенность секретного ключа, ограниченный круг поддерживаемых приложений, а также необходимость наличия сервера аутентификации [2].

Организация процессов идентификации и аутентификации

Из всего вышесказанного следует один важный вывод: надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получают доступ к защищенной информации.

Рассмотрев достоинства и недостатки некоторых методов идентификации и аутентификации, перейдем к вопросу организации данных самих процессов идентификации и аутентификации. Методика системы защиты идентификации и аутентификации является одним из приоритетных элементов инфраструктуры обеспечения безопасности от несанкционированного доступа к конфиденциальному информационному пространству. С учетом того, что всегда имеется высокий риск компрометации сетевых данных, необходимо соблюдение единых правил безопасности, в том числе при возможном сбое в процессе проверки подлинности субъекта при прохождении процедуры идентификации и аутентификации:

– нарушение конфиденциальности, целостности информационных активов неавторизованным субъектом;

– нарушение доступности при удалении важной информации из-за сбоя системы или установки вредоносного ПО;

– невозможность проверить действия авторизованных участников в результате очистки или изменения содержимого журнала событий;

– нарушение конфиденциальности, целостности, доступности информации злоумышленником, который выдает себя за другого пользователя;

Также потенциальные риски значительно возрастают при активации следующих видов атак:

– прохождение процессов аутентификации несанкционированными пользователями;

– несанкционированные изменения в базе данных с аутентифицирующей информацией (включение в базу данных несуществующего участника или изменение текущего пароля пользователя);

– перехват сессии субъекта;

– несанкционированные изменения в перечне контроля доступа к объектам системы;

– внесение изменений в систему или использование ошибок операционной системы в обход системы безопасности.

Большинство аппаратно-программных комплексов защиты реализуют максимальное число защитных механизмов. Это идентификация и аутентификация пользователей, ограничение доступа к файлам, дискам, защита процесса загрузки операционной системы и т. д. В дополнение к этим защитным механиз-

мам целесообразно также разобрать эффективные методы по противодействию несанкционированным подключениям технических устройств.

По мнению специалистов в области информационной безопасности, наиболее перспективным направлением совершенствования систем аутентификации пользователей является применение многофакторной (расширенной) аутентификации. Если сервер, на котором проводится идентификация и аутентификация, предоставляет функциональные возможности, основанные на двух «ключах», то лучше использовать эти инструменты системы безопасности в полной мере, что позволит снизить риски по компрометации вашей учетной записи, личных или корпоративных данных и иных информационных активов. При запросе двухфакторной идентификации чаще всего используют какие-либо парные сочетания: считыватель биометрической информации и пароль, смарт-карта, PIN-код и т.д. [3].

По степени безопасности субъекта аутентификации уже давно предлагалось разделить на три градации, расположенные по мере возрастания уровня защищенности:

I уровень – простая аутентификация (используется стандартная аутентификация);

II уровень – усиленная аутентификация (применяется многофакторная аутентификация, как одно из наиболее популярных доказательств механизма аутентификации);

III-уровень – строгая аутентификация (используются квалифицированные сертификаты доступа).

Вопросы надлежащей защищенности информационной среды являются весьма актуальными при попытке обеспечения безопасности в процессе идентификации и аутентификации, как частного и корпоративного пользователя, так и госслужащих и правоохранительных структур.

При выборе более высокого уровня защищенности повышается степень гарантии того, что потенциальный нарушитель не сможет пройти аутентификации от имени другого пользователя.

В роли основных рисков информационным ресурсам в системе идентификации/аутентификации, как правило, выступают: человеческий фактор, вирусы, аппаратно-программные сбои. Безусловно, человеческий фактор является самой серьезной угрозой безопасности информационной компьютерной сети, ведь общество больше всего страдает от своей деятельности, от им же созданных опасностей, причем в любой сфере деятельности [4].

Соблюдение баланса интересов граждан, общества и государства в сфере информационных технологий

Соблюдение баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов с использованием правовых, организационно-технических и экономических инструментов и способов обеспечения информационной безопасности в сфере компьютерных сетей. Очевидно, что нормальная жизнедеятельность об-

щества определяется уровнем развития, качеством функционирования и безопасностью информационной среды.

Исходя из этого утверждения нельзя не обратить внимание на последние инициативы Роскомнадзора, который предложил запрашивать паспортные данные, номер телефона, электронную почту и адрес у новых пользователей социальных сетей и мессенджеров. Инициатива родилась в рамках поправок к 152-ФЗ «О персональных данных», которые уже частично вступили в силу в марте 2021 г. [9].

По новым правилам онлайн-площадкам запретили публиковать любую личную информацию пользователей без их согласия. Речь идет о данных из социальных сетей, с сайтов объявлений и из открытых реестров. С 1 июня 2021 года они обязаны получать такое согласие либо через собственную платформу, либо через «Единую систему идентификации и аутентификации» (ЕСИА).

Порядок идентификации граждан в ЕСИА Роскомнадзор изложил в специальном Приказе. В первой версии этого документа речь шла о необходимости для пользователя вводить свои паспортные данные, телефон, адрес места жительства и электронный почты. Это вызвало волну критики. Даже если отодвинуть в сторону вопросы приватности или безопасности, то вводить такое количество данных просто неудобно. Роскомнадзор отреагировал на недовольство оперативно и сообщил, что в первую версию Приказа внесены существенные поправки. Судя по их комментариям, авторизоваться на ЕСИА можно будет через сайт госуслуг [5].

Так что, если граждане уже пользуются сайтом госуслуг, то их паспортные данные подтянутся автоматически! Для первичной же регистрации на этом сайте потребуется ввести только СНИЛС (специальный номер индивидуального лицевого счета) и телефон. Таким образом, госструктуры получают возможность связать аккаунт в соцсетях с паспортными данными его владельца. Но прямо об этом представители Роскомнадзора предпочитают не говорить!

Сама идея пускать в соцсети по паспорту не нова, она возникла еще в 2012 году. Тогда ее авторы говорили, что это нужно для того, чтобы искать нарушителей в Сети, которые прячутся за фейковыми аккаунтами. Теперь же Роскомнадзор действует исподволь, собирая информацию обходными путями. Однако с задачей деанонимизации в Интернете (если она есть) быстро не справиться.

Похоже, что чиновники Роскомнадзора забыли одну очень простую аксиому: «на каждый яд есть свое противоядие». Общеизвестно, что большинство соцсетей – иностранные, и они никогда не пойдут на поводу у российских властей. Высказывается мнение, что одним из эффектов нововведения может стать массовый отток пользователей из отечественных соцсетей.

Еще одна из претензий к инициативе Роскомнадзора касается безопасности собираемых сведений: утечки персональных данных из госструктур и банков происходят регулярно. По мнению некоторых специалистов инициатива Роскомнадзора очень вредна и губительна. Давно не секрет, что подобного рода законы соблюдают только российские площадки, иностранные их игнорируют [6].

Хочется подчеркнуть глубокую взаимосвязь всех элементов и факторов, оказывающих влияние на процессы идентификации и аутентификации. Мелочей не должно быть!

В последнее время мировой рынок программно-аппаратных средств аутентификации демонстрирует устойчивый рост, важным направлением в развитии российской системы информационных ресурсов и технологий доступа к ним является дальнейшее совершенствование методических аспектов идентификации и аутентификации.

Образно говоря, идентификация и аутентификация, как первая линия обороны, должна установить мощный заслон злоумышленникам, с целью недопущения их к конфиденциальным ресурсам, и, как следствие, обеспечить выполнение главных задач систем информационной безопасности компьютерных сетей:

– идентифицировать участников информационных процессов;

– провести аутентификацию участников информационных процессов;

– зарегистрировать участников информационных процессов;

– сформулировать перечень прошедших (не прошедших) идентификацию и аутентификацию участников информационных процессов и информационных систем [7].

Заключение

Нынешнее общество является свидетелем качественной трансформации информационных компьютерных сетей, где система идентификации и аутентификации является опорной точкой для предотвращения несанкционированного доступа к охраняемым информационным ресурсам.

Понятно, что простых и быстрых решений всех вопросов и проблем, возникающих в процессе проверки подлинности не существует. Эффективность и качество инструментов идентификации и аутентификации должны быть должным образом связаны с важностью информационных активов. При этом не следует забывать, что повышение степени безопасности, в свою очередь, сопровождается удорожанием.

Поэтому, при решении задач идентификации и аутентификации следует подходить комплексно, установив разумный баланс между эффективностью, стоимостью, удобством пользования и административным управлением средств обеспечения систем безопасности.

Британскому премьер-министру сэру Уинстону Черчиллю приписывают такую фразу: «За безопасность надо платить, а за ее отсутствие расплачиваться». Естественно, он имел в виду не компьютерную безопасность, но к рассмотренной проблеме по глубокому убеждению автора она подходит как нельзя лучше.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационная безопасность: учеб. пособие / В.В. Гафнер. — Ростов н/Д: Феникс, 2010. – 324 с.

2. Информационная безопасность: учеб. пособие / Партыка Т. Л., Попов И. И. – М.: Форум, 2012. – 452 с.

3. Информационная безопасность: учеб. пособие / Петров С. В., Слинькова И. П., Гафнер В. В. – М.: АРТА, 2012. – 296 с.

4. Информационная безопасность: учеб. пособие / Ярочкин В. И., — М.: Академический Проект; Гаудеамус, 2008. – 544 с.

5. Защита информации в компьютерных системах и сетях / Шаньгин В. Ф. – М.: ДМК Пресс, 2012. – 592 с.

6. Информационная безопасность и защита информации: учебное пособие для студ. высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под. ред. С. А. Клейменова. — 3-е изд., стер. — М.: Издательский центр «Академия», 2008. — 336 с.

7. Основы информационно-аналитической работы: учебное пособие / Левкин И. М. – Санкт-Петербург: СЗАГС, 2008. – 206 с.

8. Организация комплексной системы защиты информации: учеб. пособие / Гришина Н. В. – М.: Гелиос АРВ, 2007. – 254 с.

9. Федеральный закон №149-ФЗ. Об информации, информационных и технологиях, и защите информации. – М., 2006 с.