УДК 004.056 DOI: 10.37468/2307-1400-2020-3-59-68

МЕТЕЛЬКОВ АЛЕКСАНДР НИКОЛАЕВИЧ

О ПРОБЛЕМЕ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ПАРОЛЕЙ ПРИ ИНФОРМАЦИОННОМ ВЗАИМОДЕЙСТВИИ

АННОТАЦИЯ

Среди пользователей и специалистов не утихают споры по поводу эффективности паролей, используемых для аутентификации субъектов доступа к информационным система. Актуальность выбора темы статьи объясняется применением паролей практически в любой информационной системе, а во многих системах парольная защита используется как единственное средство. При этом стойкость пароля к вскрытию нередко определяет и безопасность всей информационной системы. Проанализированы и обобщены отечественные и зарубежные современные подходы к формированию политики паролей. На этой основе выработаны предложения по совершенствованию защиты информации с использованием паролей.

Ключевые слова: аутентификация, пароли, длина пароля, парольная политика, пользователи информационной системы, многофакторная аутентификация, криптографические методы аутентификации, алфавит пароля, строгая аутентификация, управление паролями.

METELKOV A. N.

ON THE PROBLEM OF AUTHENTICATION USING PASSWORDS IN INFORMATION INTERACTION

ABSTRACT

There is an ongoing debate among users and specialists about the effectiveness of passwords used to authenticate subjects of access to information systems. The relevance of choosing the topic of the article is explained by the use of passwords in almost any information system, and in many systems password protection is used as the only means. At the same time, the password's resistance to opening often determines the security of the entire information system. Domestic and foreign modern approaches to password policy formation are analyzed and generalized. On this basis, proposals have been developed to improve the protection of information using passwords.

Keywords: authentication, passwords, password length, password policy, information system users, multi-factor authentication, cryptographic authentication methods, password alphabet, strong authentication, password management.

Каждый пользователь современных информационных систем ежедневно сталкивается с процедурами «идентификации» и «аутентификации». Вычислительная среда, в которой функционирует критичное программное обеспечение, представляет собой доверительную платформу с аппаратным компонентом, обеспечивающим доверие между всеми участниками информационного процесса. Такой аппаратный компонент также должен обеспечивать защиту криптографических ключей и других данных, которые могут быть использованы для алгоритмов шифрования или управления доступом к серверам и сетевому оборудованию. Аутентификация всех участников информационного обмена является одним из основных механизмов безопасности, который необходимо принимать во внимание при построении доверенной вычислительной среды на базе аппаратных модулей [1, с.498]. Под аутентификацией понимают подтверждение пользователем предъявленного идентификатора, а также проверку подлинности идентификатора и его принадлежности определенному пользователю.

Существует ряд методов аутентификации, среди которых выделяют парольную аутентификацию, аутентификацию через сторонний ресурс, посредством графических паролей, с помощью одноразовых и динамических паролей, а также механизм аутентификации с использованием сторонних программных и аппаратных токенов, методы многофакторной аутентификации, криптографические методы аутентификации и биометрическую аутентификацию[3,с.16] (например, с использованием отпечатка пальца, геометрии руки и (или) лица, радужной оболочки или сетчатки глаза), аутентификацию личности по почерку и динамике написания контрольных фраз (подписи).

Самыми распространенными методами идентификации и аутентификации пользователя являются парольные системы, а также идентификация/аутентификация с использованием технических устройств и индивидуальных биометрических характеристик.

В некоторых организациях удалось добиться определенных успехов в защите паролей и предотвращении несанкционированного доступа к информации, однако еще многие сталкиваются с нерешенными вопросами в аутентификации с использованием секретного набора различных символов. Несмотря на широкое внедрение многофакторной аутентификации, продолжается использование плохих практик парольной политики, препятствующих эффективному государственному и корпоративному управлению в достижении современных стандартов информационной безопасности и технической защиты информации. В своем интервью 29 июня 2020 г. журналисту в рамках спецпроекта ТАСС «Первые лица бизнеса» глава Сбербанка России Г.Грефф по результатам анализа инцидента, связанного с утечкой конфиденциальной банковской информации через возможности подготовленного внутреннего нарушителя, сообщил, что Сбербанк изменил парадигму защиты с «системы могут быть уязвимыми» на «сделаем свои системы абсолютно неуязвимыми изнутри». Одной из кардинальных мер в ее реализации явилось резкое сокращение числа администраторов, имевших доступ к конфиденциальной клиентской информации [2].

Пароль (password) представляет собой строку символов (букв, цифр и других символов), используемых для проверки подлинности удостоверения или авторизации субъекта доступа. Паролем согласно руководящему документу «Защита от несанкционированного доступа к информации. Термины и определения», утвержденному решением председателя Гостехкомиссии России от 30 марта 1992 г., называется «идентификатор субъекта доступа, который является его (субъекта) секретом». Особая разновидность пароля – парольная фраза, то есть последовательность слов или иной текст. Простой пароль обладает негарантированной стойкостью к вскрытию, однако обладает рядом привлекательных для пользователя свойств: простотой формирования, легким запоминанием, произвольной длинной. Сложные пароли являются случайной выборкой символов из алфавита определенной последовательности (A), формирующая их последовательность по скрытому алгоритму (L) в набор длины (S), обоснованной для соответствующего уровня стойкости к вскрытию[4, с.71]. Метод парольной защиты уязвим, т.к. пароль, как правило, является отчуждаемым от своего владельца [6, с.130].

Тема парольной защиты получила подтверждение своей актуальности в связи распространением 11 июня 2020 года в сети Интернет журналистских материалов с названием «Полковника подвел пароль» [8]. Как сообщается в газете «Коммерсантъ» (Приволжье, Нижний Новгород) с помощью одного из бывших руководителей отдела оперативно-розыскной информации нижегородской полиции С., некоммерческая организация предоставляла банкам и предприятиям служебную информацию о персональных данных граждан, адресах их прописки, сведениях о судимости, номерах машин. По закрытым шифрованным каналам на базе программного обеспечения VipNet личными данными обменивались полиция и другие госорганы, а также службы безопасности нижегородских банков и многих крупных предприятий. Частные клиенты вносили ежемесячную абонентскую плату. Как правило, бизнес с помощью АНО проверял заемщиков, контрагентов или резюме соискателей работы, запрашивая справки на граждан с их персональными данными, наличием или отсутствием у них судимостей и правонарушений. Постоянно накапливающийся банк данных «Центра информационно-аналитической и правовой поддержки органов исполнительной власти и правоохранительных структур» работал до тех пор, пока в 2013 году эта деятельность не привлекла внимание спецслужб. Некоммерческая организация для обеспечения взаимодействия заключила межведомственные соглашения с различными органами власти и силовыми структурами по обмену межведомственной информацией.

После проверки соблюдения режима секретности сотрудниками территориального органа безопасности сервер АНО был убран из помещения областного управления МВД. Руководство Центра решило прекратить свою деятельность. В 2016 году по уголовному делу был арестован С., уволившийся из полиции и работавший в АНО заместителем директора по развитию. Согласно версии следствия, действия С. привели к тяжким последствиям из-за получения коммерческими компаниями служебной информации. Осужденный считает обвинение недоказанным. По его словам журналисту, он открыто заходил в базу данных под своим логином и паролем (после увольнения из полиции остались действующими его учетные данные), а не занимался какими-либо тайными взломами или несанкционированным вмешательством в информационные системы. Суд признал С. виновным по ч. 2 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и приговорил его к трем годам лишения свободы условно. К сожалению, как свидетельствуют решения судебных органов по неправомерному доступу к компьютерной информации, подобная ситуация не является каким-либо исключительным явлением. Рассмотренный пример показывает важность точного определения прав и порядка работы с информационными ресурсами различных субъектов для недопущения неправомерного доступа при изменении обстоятельств.

Многообразие атак на систему парольной защиты средств вычислительной техники организации повышает шансы злоумышленника получить удаленный доступ к конфиденциальным данным, хранящимся в информационной системе. Пароль может быть подобран путем перебора всех возможных комбинаций входящих в него символов, перехвачен при его передаче пользователем в информационную систему или при осуществлении операции сравнения и отождествления. Подготовленный нарушитель способен проникнуть в область памяти, в которой хранятся эталонные пароли. Защититься от таких угроз возможно путем последовательной политики выбора трудно раскрываемых паролей.

В методическом документе «Меры защиты информации в государственных информационных системах», утвержденном ФСТЭК России 11 февраля 2014 г., рекомендуется при доступе в информационную систему осуществлять идентификацию и аутентификацию пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от их имени, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям отнесены пользователи и администраторы, выполняющие свои обязанности с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами, утвержденными оператором. В информационной системе таким пользователям присвоены учетные записи. В качестве внутренних пользователей кроме того рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения ремонта, гарантийного обслуживания, регламентных и иных работ в соответствии с организационно-распорядительными документами оператора, и которым в информационной системе также присвоены учетные записи. Пользователи системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации.

Меры защиты информации, включая идентификацию и аутентификацию субъектов доступа и объектов доступа, реализуются в информационной системе в рамках ее системы защиты информации в зависимости от класса защищенности информационной системы, угроз безопасности информации, структурно-функциональных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования информационной системы.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных

средств, биометрических характеристик, иных средств или в случае многофакторной аутентификации – определенной комбинации указанных средств. Многофакторной аутентификацией считается технология контроля доступа, при которой кроме ввода логина и пароля к аккаунту пользователя субъекту доступа необходимо подтвердить свою личность дополнительными способами.

Оператором должны быть установлены и реализованы функции управления средствами аутентификации пользователей и устройств в информационной системе. К ним относятся установление характеристик пароля (при использовании механизмов аутентификации на основе пароля) путем задания:

- минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
- минимального количества измененных символов при создании новых паролей;
- максимального и минимального времени действия пароля, а также запрета на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей.

В случае применения в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны удовлетворять следующим рекомендациям регулятора. При длине пароля не менее 6 символов, алфавите пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки должно составлять от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации должна составлять от 3 до 15 минут. Смена паролей при этом должна осуществляться не более чем через 180 дней. Если длина пароля составляет не менее 6 символов, алфавит пароля – не менее 60 символов максимальное количество неуспешных попыток аутентификации до блокировки должно составлять от 3 до 10 попыток. Блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации должна происходить в течение 5–30 минут. Смена паролей должна осуществляться не более чем через 120 дней. При длине пароля не менее 6 символов, алфавите пароля не менее 70 символов, максимальное число попыток ввода неправильного пароля до блокировки должно составлять от 3 до 8 попыток за промежуток времени от 10 до 30 минут. Смена паролей должна осуществляться не более чем через 90 дней. При длине пароля не менее 8 символов, алфавите пароля не менее 70 символов максимальное количество неуспешных попыток аутентификации до блокировки от 3 до 4 попыток при достижении установленного максимального количества неуспешных попыток аутентификации должно составлять от 15 до 60 минут. Смена паролей должна происходить не более чем через 60 дней.

В информационной системе должно быть обеспечено использование: -автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости механизма аутентификации и для оценки характеристик этих механизмов; - серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах информационной системы и компонентах программного обеспечения, предусматривающего собственную аутентификацию. Оператор должен запросить у поставщика технических средств и программного обеспечения информационной системы аутентификационную информацию, заданную производителем этих технических средств и программного обеспечения и не указанную в эксплуатационной документации. Оператором должны быть определены меры по исключению возможности использования

пользователями их идентификаторов и паролей в других информационных системах.

Вместе с тем специалисты ИТ-компании «Азон» отмечают наметившуюся тенденцию в желании пользователей отказаться от использования паролей. В частности, как «показывает статистика, 84% пользователей не против отказаться от паролей, как средства доступа к важной информации». Одним из надежных способов обеспечения безопасности является биометрическая аутентификация. Большинство опрошенных респондентов выступили за использование альтернативной формы верификации, например, путем сканирования отпечатков пальца [5]. К примеру, сканирование отпечатка пальца избавит пользователя от набора цифр и символов в пароле, и, соответственно, от его забывания, утери и, тем более, передачи другому человеку.

Метод аутентификации на основе паролей применяется в системах управления доступом посредством реализации решений, направленных на автоматизацию процесса идентификации пользователя, разграничения его прав и контроля доступа.

Пароли используются многими способами для защиты данных, систем и сетей. Например, пароли применяются для аутентификации пользователей операционных систем и приложений, таких как электронная почта, трудовая запись, удаленный доступ и т.д. Биометрическое устройство может генерировать пароль на основе сканирования отпечатков пальцев, и этот пароль затем используется для аутентификации. Пароли также используются для защиты файлов и другой хранимой информации, например пароля для защиты одного сжатого файла, криптографического ключа или зашифрованного жесткого диска.

В решении проблемы аутентификации существует несколько подходов для обеспечения безопасности цифровой информационной инфраструктуры. Распространённым методом является двухфакторная аутентификация, в том числе на основе одноразовых паролей. В отдельных случаях пароли используются без идентификатора пользователя. Такой подход весьма часто встречается в ситуациях с низким уровнем безопасности (например, при вводе цифрового кода в офисный копировальный аппарат). Для реализации надежного механизма защиты доступа к информационным ресурсам применяются решения с использованием строгой и двухфакторной аутентификации. В большинстве практических реализаций пароль связан с идентификатором пользователя. При таком подходе после предоставления идентификационных данных, для подтверждения своей подлинности пользователю или устройству необходимо предъявить дополнительно одноразовый пароль, генерируемый центром распределения ключей. Изложенный метод не требует от устройств дополнительных вычислительных ресурсов или хранилищ, однако является неприемлемым для устройств, не способных поддерживать процедуру ввода полученного одноразового пароля. Аналогично можно сказать и о методе аутентификации, вторым фактором которого является аппаратный идентификатор.

Строгая аутентификация подразумевает использование двух факторов аутентификации различных типов. Первый фактор – наличие токена или смарт-карты, второй – PIN-код для совершения криптографических операций, непосредственно, внутри устройства (токен, смарт-карта). Для обеспечения доступа к системе с критически важной информацией, целесообразно применение дополнительного фактора аутентификации – идентификации пользователя с помощью биометрических данных. В этом случае, использование токена без его владельца затруднительно.

В качестве средств аутентификации используют статические (отпечатки пальцев, геометрию руки или лица, радужную оболочку и/или сетчатку глаза) и динамические характеристики. Использование технологии отпечатков пальцев в качестве фактора аутентификации обеспечивает новый уровень информационной безопасности организации. В случае подделки, физического насильственного отделения частей от человека для последующего использования эта уязвимость может быть компенсирована использованием динамических биометрических характеристик [7]. Использование

технологии отпечатков пальцев в качестве фактора аутентификации обеспечивает повышенный уровень информационной безопасности организации, однако требует соблюдения норм Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, с осуществлением правосудия и исполнением судебных актов, с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве, уголовно-исполнительным законодательством, .

Особенностями биометрической аутентификации являются:

- замена сложных и длинных паролей отпечатком пальца (пальцев);
- обеспечение совместимости с другими системами информационной безопасности;
- не связанность с формированием биометрическую базу данных;
- неотчуждаемость в отличии от USB-токенов или смарт-карт.

Специалисты по информационной безопасности в нашей стране и за рубежом высказывают мнения о нецелесообразности в современных условиях осуществления аутентификации по паролю. Свое мнение ими мотивируется не соответствием данного метода доступа субъектов к данным, подлинность которого проверяется паролем, растущим требованиям безопасности и неудобством для пользователей. Главный недостаток парольной аутентификации заключается в возможности передачи пароля другому лицу. На практике это происходит весьма часто. В личной жизни от такого поступка может пострадать сам пользователь. В корпоративных сетях компаниям может быть причинены репутационные потери и финансовый ущерб, наступить негативные юридические последствия. В числе других недостатков парольной аутентификации является использование одного и того же пароля для осуществления доступа к совершенно разным системам –как к личным аккаунтам на сайтах, так и в корпоративной сети. При этом пользователи обычно осознают, что такой подход категорически противопоказан для защиты конфиденциальной информации. Утечка пароля, в таких случаях, может навредить информации, хранящихся сразу на нескольких ресурсах. Недостатком является и привычка (оценкам до 77% опрошенных пользователей) записывать пароли на бумажках. В основном, на такие поступки их побуждают сайты и многочисленные системы, которые в целях безопасности, периодически требуют заменить пароль, или приглашают пользователей формировать пароль по предлагаемым шаблонам. В этой связи руководителям организаций, ИТ-отделов и служб безопасности уместно рассмотрение и уточнение парольной политики.

Знание основ технологий идентификации, включая управление паролями, способы единого входа и многофакторной аутентификации позволяет руководителям предприятий и организаций углубить понимание проблем, рисков и приоритетов, связанных с управлением идентичностью на современном рабочем месте оператора информационных систем. Такое знание может побудить к совершенствованию мер противодействия неправомерному доступу к компьютерной информации в организации.

Пароли сами по себе означают повышенный уровень безопасности, который помогает пользова-

телю войти в различные служебные базы данных, сайты социальных сетей, получить доступ к своим сетевым банковским услугам с помощью простого пароля аутентификации, созданного самим пользователем. Как показывает отечественная и зарубежная практика, пароли, созданные пользователем, не всегда безопасны, так как обычному человеку запоминать сложные пароли не просто.

Специалистами разработаны комбинированные схемы управления паролями пользователя с помощью аутентификации OTP, объединенной с буквенно-цифровым мастер-паролем. Такая модель делает несложной фиксацию в памяти, а также обладает вычислительной мощью. Алгоритм OTP делает конечный буквенно-цифровой токен допустимым для сеанса и для одноразового использования. Менеджер паролей предоставляет простой способ проверки подлинности системы, который позволяет пользователю не обязательно запоминать какие-либо сложные пароли или комбинации символов [10]. Конкатенация аутентификации OTP и менеджера паролей отсутствует.

Внедрение отечественных технологий в цифровизацию различных сфер человеческой деятельности связано с учетом зарубежного опыта, в частности, американской организации NIST. В 2017 году NIST представила рекомендации по паролям, принятие которых резко возросло в 2019 году, поскольку они получили одобрение экспертов по безопасности во всем мире. В рекомендациях сбалансированы удобные для пользователя политики паролей, направленные на повышение безопасности и снижение затрат.

Для реализации руководящих принципов NIST password standards, организации используют инструменты автоматизации проверки открытых паролей и применяют политики паролей. Автоматизированные политики паролей упрощают выполнение рекомендаций по паролям, не создавая большой дополнительной нагрузки на ИТ-специалистов. Когда существующий пароль становится уязвимым, действия по исправлению выполняются автоматически, а не требуют ручного вмешательства администратора или службы поддержки. Организации должны также учитывать применимые в государстве мандаты (например, FISMA в США), правила, требования и руководящие принципы, связанные с паролями.

Генеральный директор компании по кибербезопасности CEO & GM, Enzoic (ранее называлась PasswordPing) Майк Грин (Mike Greene) для приведения в соответствие требованиям NIST рекомендует четыре варианта автоматической политики паролей:

– непрерывный мониторинг открытых паролей;
– защита от часто используемых паролей;
– блокирование ожидаемых или аналогичных паролей;
– запрещение использования контекстно-зависимых паролей.

По данным Verizon DBIR, скомпрометированные пароли ответственны за 81% нарушений, связанных с хакерством. Непрерывный мониторинг открытых паролей позволяет выявить признаки возможной хакерской деятельности на ранней стадии реализации актуальных угроз безопасности информации. Как отмечает М.Грин, среднестатистический человек 13 раз повторно использует один и тот же пароль [9]. Киберпреступники полагаются на это небрежное поведение и охотятся за уязвимостями, вызванными повторным использованием паролей. Однако во многих случаях сокрытие идентификаторов бесполезно, поскольку они основаны на адресе электронной почты пользователя, имени и фамилии или другой информации, легко доступной злоумышленникам. Если пользователь использует один и тот же пароль в нескольких системах, наличие разных идентификаторов снижает вероятность того, что злоумышленник, получивший пароль пользователя в одной системе, сможет повторно использовать его в других системах.

ИТ-подразделения и службы безопасности борются с постоянно обновляющимся черным списком паролей путем проверки паролей. Однако злоумышленники совершенствуют технологии для несанкционированного воздействия. Если в организации применяет только старые черные списки паролей, они расширяют окно атаки для получения

злоумышленниками учетной записи сотрудника. NIST рекомендует осуществлять непрерывный скрининг паролей для своевременного выявления этого вектора атаки. В специальной публикации NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations» определен ряд средств контроля безопасности, непосредственно связанных с идентификацией и аутентификацией. В соответствии с NIST SP 800-53 минимальные требования к паролям варьируются в зависимости от уровня «Федеральные стандарты обработки информации» (FIPS 199).

В связи с тем, что некоторые пользователи нередко используют слабые, распространенные пароли и не знают об этом, часто используемые пароли следует экранировать от них. Для этого применяется практика автоматизированной проверки паролей, начиная с предотвращения употребления обычных слов. Сопряжение общих слов с другими словами, специальными символами и числами может быть разрешено только при соответствующей длине символов. Кроме того, организации должны блокировать повторяющиеся или последовательные символы. Существует также множество наиболее распространенных паролей, о возможном использовании которых некоторыми пользователями известно злоумышленникам, поэтому организации должны блокировать общие пароли (например: 123456, qwerty, abc123, password1).

Блокирование ожидаемых или аналогичных паролей является необходимой мерой защиты, так как большинство сотрудников также повторно используют пароли в виде корневого пароля, который изменяется с помощью простой замены цифр буквами. Злоумышленники знают такую обычно сложившуюся практику, поэтому организациям необходимо принимать меры для предотвращения использования сотрудниками ожидаемых паролей и их различных форм. Нечеткое сопоставление очень важно, потому что, если пароль пользователя недавно был открыт в интернете с другого сайта, злоумышленник может использовать шаблоны этого пароля. Нечеткое соответствие пароля проверяет наличие нескольких вариантов пароля, включая чувствительность к регистру, а также общие замены, такие как leetspeak и реверсирование пароля. Например: в случае использования открытого пароля – «HolidayVacation1» злоумышленники обычно пытаются использовать такие варианты, как: «HolidayVacationi» Leetspeak (подставляя цифры вместо букв типа leet = 1337), «1noitacaVyadiloH» обратный пароль «holidayvacation1» изменение с учетом регистра. Другим типичным случаем является использование одного пароля root, а затем изменение только одного или двух символов. Подобная практика облегчает сотруднику запоминание пароля, но, к сожалению, она также позволяет злоумышленникам легко угадать его. При блокировке сходства паролей новые пароли экранируются по сходству с предыдущим паролем с помощью расстояния Дамерау-Левенштейна. Злоумышленники обычно пробуют итерации скомпрометированного пароля путем изменения одного, двух символов или осуществляют их двузначное изменение. Системный администратор должен быть способен определить расстояние между старым и новым паролями. При использовании этой политики паролей минимальное количество различий символов должно быть не менее одного.

У специалистов есть разные мнения о том, на сколько символов должны отличаться старые и новые пароли, поэтому важно, чтобы пользователи выбрали инструмент настройки паролей. Рецепт хорошего пароля, по мнению специалистов, заключается в его длине: чем длиннее пароль и разнообразнее символы, тем больше времени занимает полный перебор.

Запрещение использования контекстно-зависимых паролей объясняется тем, что нарушители могут попытаться использовать контекстно-зависимые пароли для получения доступа к учетным записям Active Directory. Злоумышленники знают, что сотрудники могут включать название своей компании или продукта в свой пароль. Для борьбы с этим компаниям необходимо создать фильтр для пользовательского словаря паролей с возможностью добавления пользовательских локальных паролей, которые

будут проверяться и блокироваться при создании. Пользовательские пароли могут быть частично совпадающими и нечувствительными к регистру, поэтому любой пароль, содержащий это слово, будет заблокирован. Например, если словарь паролей клиентов содержит слово «GeneralElectric», пользователям не будет разрешено использовать это слово в любом пароле, поэтому пароль типа» ILovegeneralElectric « будет заблокирован.

Организации нуждаются в быстром развертывании принудительного применения политики паролей и ежедневной проверке открытых паролей, которая автоматизирована для уменьшения дополнительной нагрузки на специалистов информационной безопасности. Автоматизация позволяет настроить политики паролей и обеспечивать их работу. При выявлении уязвимости существующего пароля, действия по его исправлению выполняются автоматически и не требуют ручного вмешательства администратора или службы поддержки. Автоматизированная фильтрация слабых паролей, нечеткое сопоставление паролей, блокировка сходства паролей и фильтрация пользовательских словарей паролей позволяют организациям быстро и легко принимать требования NIST к паролям. В организациях также проверяются логины на наличие скомпрометированных учетных данных для предотвращения их захвата и последующих угроз.

Управление паролями представляет собой процесс определения, внедрения и поддержания политик паролей на всей территории организации. Эффективное управление паролями максимально снижает риск компрометации систем аутентификации на основе паролей. Организации заинтересованы в защите конфиденциальности, целостности и доступности паролей. Они должны обеспечить такой режим, чтобы все авторизованные пользователи могли успешно использовать пароли по мере необходимости и ни один неавторизованный пользователь не имел бы несанкционированного доступа. Целостность и доступность должны быть обеспечены средствами контроля безопасности данных, такими как использование списков контроля доступа для предотвращения перезаписи паролей злоумышленниками и создание защищенных резервных копий файлов паролей.

Обеспечение конфиденциальности паролей является сложной задачей и включает в себя наряду с решениями, касающимися характеристик самих паролей, меры по обеспечению безопасности. Например, требование, чтобы пароли были длинными и сложными, снижает вероятность того, что злоумышленники догадаются или взломают их. Однако это требование также затрудняет запоминание паролей пользователями и, следовательно, повышает вероятность небезопасного хранения. В результате увеличивается вероятность хранения паролей пользователями небезопасным способом и использования условий, способствующих реализации угроз со стороны злоумышленников.

Выводы

1. Защита конфиденциальности идентификаторов пользователей методом затруднения проведения злоумышленникам целенаправленных атак требует реализации мер по сокрытию имен пользователей. Для обеспечения безопасности от возможных актуальных целенаправленных атак целесообразно использовать уникальные идентификаторы.

2. Использование различных идентификаторов имеет ограниченное значение для безопасности, поскольку многие угрозы связаны с захватом идентификаторов вместе с паролями. Следует учитывать, что пользователи вынуждены запоминать каждый идентификатор или записывать идентификаторы в легко доступном месте.

3. Процесс управления паролями должен быть отрегулирован на уровне организации, в которой используется цифровая информационная инфраструктура, связанная с автоматизированной обработкой конфиденциальной информации. В такой организации важно разрабатывать политику паролей, определяющую все требования по управлению паролями.

4. Политика паролей организации должна учитывать возможности паролей, предоставляемые различными операционными системами и приложениями. Например, алгоритмы шифрования и

наборы символов паролей, которые они поддерживают, могут отличаться. Для учета возможностей паролей, предоставляемых различными операционными системами и приложениями, политика безопасности должна быть гибкой, содержать требования по хранению и передаче паролей, составлению паролей, а также процедуры выдачи и сброса паролей. Политика паролей должна также учитывать защиту паролем, обеспечиваемую различными механизмами, и компенсирующие меры контроля, которые могут потребоваться для устранения недостатков в этих механизмах.

5. В случае технологических изменений, способных повлиять на управление паролями, политика паролей должна периодически пересматриваться. При этом средства контроля безопасности, связанные с паролями, должны уточняться для обеспечения совместимости с действующей политикой паролей организации.

После разработки политики паролей организации должны выбирать элементы управления безопасностью, реализующие такую политику.

Список литературы

1. *Гатчин Ю.А., Теплоухова О.А.* Алгоритм аутентификации участников информационного взаимодействия при удаленной загрузке операционной системы на тонкий клиент // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Том 16. – № 3. – С.497-505.
2. Герман Греф: я – игрок в долгую. 29 июня 2020 г. [Электронный ресурс]. – Режим доступа: https://tass.ru/business-officials/8827375 (дата обращения 03.07.2020)
3. *Комарова А.В.* Методы повышения безопасности комбинированных схем аутентификации. Дисс. …. кан. технич. наук. Специальность: 05.13.19. – СПб, 2019. – С.16.
4. Введение в информационную безопасность: Учебное пособие для вузов / А. А. Малюк, В. С. Горбатов, В. И. Королев и др.; Под ред. В. С. Горбатова. – М.: Горячая линия – Телеком, 2018 – 288 с.
5. Пользователи хотят отказаться от паролей [Электронный ресурс]. – Режим доступа: https://www.azone-it.ru/polzovateli-hotyat-otkazatsya-ot-paroley (дата обращения 9.06.2020)
6. *Сулавко А.Е., Жумажанова С.С., Фофанов Г.А.* Перспективные нейросетевые алгоритмы распознавания динамических биометрических образов в пространстве взаимосвязанных признаков // Динамика систем, механизмов и машин. – 2018. – Том 6. – № 4. – С.130.
7. *Шелупанов А.А., Евсютин О.О., Конев А.А. и др.* Актуальные направления развития методов и средств защиты информации // Доклады ТУСУР. – 2017. – Т. 20. – № 3. – С. 15
8. *Яровицын Р.* Полковника подвел пароль: Андрея Солдаткина осудили за неправомерный доступ к информации МВД // Коммерсантъ (Н.Новгород) №101 от 09.06.2020. с.8. [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/4373270 (дата обращения 10.06.2020).
9. *Greene, Mike.* 4 Automated Password Policy Enforcers for NIST Password Guidelines. Automate Screening of Exposed Passwords and Password Policy Enforcement, November 15, 2019. [Электронный ресурс]. – Режим доступа: https://www.bankinfosecurity.com/blogs/enzoic-blog-3-6-x2-p-2803 (дата обращения: 13.08.2020).
10. *Pandey, Dr.Anand.* Password Management Using OTP Authentication // International Journal Of Advanced Research In Engineering Technology & Sciences. – 2015. – Vol. 2. – Is.3. – p.101-105. [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/292148986_Password_Management_Using_OTP_Authentication.

Статья поступила в редакцию 14 августа 2020 г.
Принята к публикации 21 сентября 2020 г.

Ссылка для цитирования: Метельков А.Н. О проблеме аутентификации с использованием паролей при информационном взаимодействии // Национальная безопасность и стратегическое планирование. 2020. № 3(31). С. 59-68. DOI: https://doi.org/10.37468/2307-1400-2020-3-59-68