

ЗАЩИТА УЧЁТНЫХ ЗАПИСЕЙ

КАК ОБЕСПЕЧИТЬ СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ В ФИНАНСОВОЙ СФЕРЕ?



**Михаил
РОЖНОВ**
технический
директор
MFASOFT

Защита учётных записей — одна из ключевых областей успешной практики информационной безопасности, а также предмет нормативных требований. Разберём требования PCI DSS 4.0 и ГОСТ 57580 к защите учётных записей, а также то, как выполнить их с помощью российского программного комплекса Secure Authentication Server компании MFASOFT.

Большинство взломов происходят из-за компрометации пользовательских учётных записей, и именно поэтому к их защите подходят с большим вниманием. Однако при выборе комплексной стратегии ИБ в финансовых организациях возникает вопрос: на какой из стандартов стоит ориентироваться в первую очередь?

Чтобы ответить на него, нужно разобраться, чем отличаются требования самых важных стандартов информационной безопасности в финансовой сфере: отечественного ГОСТ 58570 и международного PCI DSS в редакции 4, которая пока не переведена официально на русский язык. Заметно, что при создании ГОСТ 57580 специалисты ориентировались на приказы ФСТЭК 17 и 21, а также явно повторили основные положения PCI DSS. Поэтому большинство решений, для которых выполняются требования PCI DSS, будут соответствовать ГОСТ 57580 и наоборот. Но есть и различия.

КАКОЙ СТАНДАРТ СТРОЖЕ?

Оба стандарта определяют одни и те же факторы доступа к учётным записям: знание (например, пароль), владение (например, токен) и биометрия. Однако PCI DSS разделяет многофакторную и многоэтапную аутентификацию. Для входа в систему пользователь должен предоставить два или более факторов, причём разной природы, но если пользователь видит результат проверки фактора после каждого этапа, то согласно PCI DSS это уже не

многофакторная, а многоэтапная аутентификация.

Также оба норматива подразумевают наличие уникальных учётных записей, хотя использование общих аккаунтов PCI DSS в отдельных случаях допускает. Хранение и передача учётных данных в открытом виде запрещены по ГОСТ 57580, а PCI DSS требует надёжной криптографии, то есть использования принятых и проверенных отраслью алгоритмов с эффективной стойкостью ключа не менее 112 бит и надлежащими практиками управления ключами.

Кроме этого, в PCI DSS предусмотрено специальное требование для сервис-провайдеров, которые обслуживают сразу несколько систем: им необходимо вести уникальный фактор для каждой системы. Оба стандарта предписывают блокировать на 30 минут доступ в систему при неудачных попытках входа. В PCI DSS ограничение количества попыток — 10, тогда как ГОСТ 57580 оставляет этот параметр на усмотрение администратора. Стандарты также предписывают протоколирование процессов аутентификации и длительное хранение событий для возможного анализа.

Пересмотр прав пользователей по требованиям обоих стандартов должен производиться регулярно — в среднем не реже 1 раза в 6 месяцев. Но если PCI DSS призывает ориентироваться на активность учётных записей, то ГОСТ 57580 предписывает сопоставлять учётные записи с реальным персоналом и отключать аккаунты для уволенных сотрудников и подрядчиков, закончивших свою работу.

Однако, когда речь идёт о выборе пароля, более подробные и слож-

Чтобы соответствовать требованиям обоих стандартов, в большинстве аспектов можно полагаться на более строгие требования PCI DSS, а в вопросах выбора пароля лучше реализовать положения ГОСТ 57580

ные требования предъявляет именно ГОСТ 57580. В положениях PCI DSS указано, что пароль должен быть не менее 12 символов, тогда как ГОСТ требует 16 символов и задаёт разные параметры для разных групп, что реализовать сложнее. PCI DSS предписывает использовать буквы и цифры, ГОСТ 57580 — также символы и буквы разного регистра. Дополнительно по положениям ГОСТ 57580 пароль не должен быть легко вычисляемым и не должен повторять ни один из предыдущих.

Таким образом, чтобы соответствовать требованиям обоих стандартов, в большинстве аспектов можно полагаться на более строгие требования PCI DSS, а в вопросах выбора пароля лучше реализовать положения ГОСТ 57580.

КАК ВЫПОЛНИТЬ ТРЕБОВАНИЯ?

Сейчас одним из важнейших разделов требований к защите учётных записей является многофакторная аутентификация (multi-factor authentication, MFA). В PCI DSS версии 4 она обязательна для неконсольного доступа администраторов и для любого доступа к CDE (Cardholder Data Environment, среда данных держателей карт). Согласно ГОСТ 57580 она требуется для аутентификации эксплуатационного персонала, а также для всех пользователей, имеющих удалённый доступ.

Все эти требования можно реализовать при помощи доступных на российском рынке коробочных программных продуктов. Рассмотрим, как эту задачу решает программный комплекс Secure Authentication Server (SAS) компании MFASOFT. SAS — полностью российское решение, входит в реестр российского ПО. SAS имеет сертификат ФСТЭК по 4-му уровню доверия, что делает продукт одним из наиболее подходящих для реализации требований обоих стандартов.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ «ИЗ КОРОБКИ»

SAS уже сегодня используется в российских компаниях, обеспечивая со-

ответствие самым строгим требованиям стандартов за счёт встроенных в него функций. Разберём его возможности на примерах конкретных положений PCI DSS.

Пункт 8.2.1. Все действия пользователей должны относиться к уникальному субъекту. Все субъекты доступа в SAS имеют уникальный идентификатор, поэтому любая операция однозначно определяет субъект доступа.

Пункт 8.2.2. Все действия, выполняемые пользователями с генерируемыми, системными или общими идентификаторами, должны однозначно определять субъект доступа. В качестве дополнительного фактора идентификации субъекта используется уникальный номер аутентификатора.

8.2.4. События жизненного цикла для идентификаторов пользователей и факторов аутентификации не должны происходить без соответствующего разрешения. SAS содержит встроенные механизмы аутентификации при доступе к консоли администрирования, ограничения для администраторов (IP-адреса, дни недели), разграничение доступа на уровне тенантов (виртуальных серверов) и разделов консоли администрирования.

Пункт 8.2.5. У пользователей, отношения с которыми прекращены, доступ должен быть немедленно отозван. SAS периодически выполняет синхронизацию по LDAP через специальный программный агент. Пользователи, которые заблокированы в каталоге LDAP или у которых истёк срок действия учётной записи, помечаются в системе как заблокированные. Также можно вручную или через правила ограничить срок действия учётной записи или группы.

Пункт 8.2.6. В случае неактивности субъекта доступа более 90 дней

он должен быть удалён или заблокирован. В SAS можно установить автоматическую блокировку учётной записи, если она долго не используется. Дополнительно можно настроить автоматический отзыв токенов у заблокированных пользователей, что позволяет не только выполнять требования стандарта, но и экономить на стоимости лицензий, если выбрана модель оплаты по фактическому использованию.

Пункт 8.3.1. Доступ к объекту не должен быть предоставлен без указания пользовательского идентификатора и фактора аутентификации. SAS проверяет один или несколько факторов. Аутентификаторам можно назначать ПИН-код, и тогда при входе нужно вводить динамический пароль, состоящий из ПИН-кода и одноразового пароля, представляющих разные факторы.

Пункт 8.3.3. Неавторизованный пользователь не может получить доступ к системе, выдав себя за другого авторизованного субъекта доступа. SAS позволяет заново инициализировать факторы аутентификации, для которых нужно подтвердить личность пользователя, включая сброс ПИН-кода или перевыдачу токенов.

Пункт 8.3.4. Фактор аутентификации не может быть угадан атакой brute force. SAS позволяет временно блокировать учётную запись при попытках перебора и автоматически разблокировать её через определённый интервал времени.

Пункт 8.3.11. Фактор аутентификации не может быть использован кем-то ещё, кроме субъекта, которому он был назначен. Для этого в SAS для аутентификаторов отдельных типов можно задать ПИН-код, известный только владельцу токена.

Подробнее о компании MFASOFT
и программном комплексе
Secure Authentication Server:
<https://mfasoft.ru>

