Стандарт управления учетными записями и правами доступа

Иван КОРЕШКОВ,
менеджер по продукту Ankey IDM компании «Газинформсервис»

На протяжении нескольких лет продолжалась совместная деятельность разработчиков и регуляторов в сфере стандартизации класса решений, известного как Identity Management, или Identity Governance and Administration (IdM/IGA). Пока подобного стандарта не существовало, представленные на российском рынке решения создавали, основываясь на обратной связи заказчиков и с учетом их пожеланий. Что представляют собой требования, установленные обновленным ГОСТ Р 71753-2024?

В ранних версиях проекта этого стандарта были приведены довольно общие термины и определения. Впоследствии каждый из производителей этого класса решений вносил сотни пожеланий к документу, чтобы регулятор привел все уточнения к общему знаменателю. А поскольку компаний – участников ТК-362 (технического комитета по стандартизации «Защита информации») много, то объем совместной работы был колоссальным.

Набор функций

Основной аспект, который рассматривает ГОСТ, – совокупность функций, которыми должен быть наделен IdM. В основе – управление учетными записями, полномочиями, рисками доступа и контролем ролевой модели (RBAC). Поскольку такие решения способны хранить большой набор данных, часть из которых могут являться персональными (ПДн), то последняя версия стандарта, принятая 20 декабря 2024 г., регламентирует хранение таких наборов, а точнее – его недопустимость.

Следует отметить, что к ПДн можно отнести даже сочетание ФИО и электронной почты частного лица, поэтому использование таких идентификаторов ограничивается. Некоторые IdM-решения на российском рынке, например, Ankey IDM, отличаются способностью глубокого разграничения доступа к наборам данных.

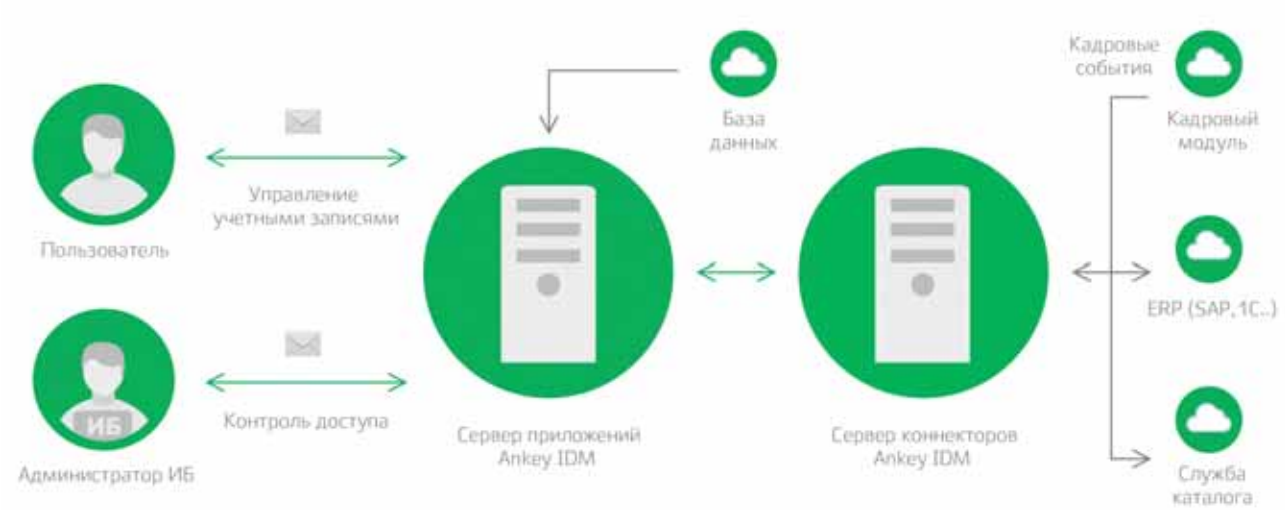
Основной аспект, который рассматривает ГОСТ, – совокупность функций, которыми должен быть наделен IdM.

Сфера применения

Второй аспект, который затрагивает стандарт, – области применения. Совместно с регулятором приняты такие общие понятия, как статус сотрудника, его учетные записи, роли, трудоустройство. При этом предусматривается возможность расширения многих объектов и областей.

Документом введено понятие «единый каталог пользователей». Собственно, это малая толика задач современного IdM-решения, которое обрело статус стандартизированного.

С каталогом пользователей неразрывно связаны и правила его наполнения, и обновления на основании данных, полученных из доверенного источника (ДИ – система или несколько систем, где ФИО, должность и другие данные сотрудника заполняются в первую очередь). Описывается и логика работы IdM по умолчанию.



Пароли и шифрование

Еще один значимый аспект, описанный в стандарте, – парольные политики, которые распространяются на автоматическое предоставление доступа. В то же время ряд требований к возможности передачи паролей (например, при передаче сотруднику впервые) относятся к избыточным. Особый акцент по какой-то причине делается на пин-конвертах (технологии передачи, аналогичной получению пин-кода вместе с банковской картой). Подобные технологии используются в ограниченном числе компаний.

Непосредственно с хранением данных связано их обязательное шифрование. При этом стандарт затрагивает только способ хранения паролей. Хотя известны вендоры, которые шифруют данные полностью: от данных сотрудников до механизмов согласования и, тем более, паролей (в случае их хранения). В таких решениях в последние несколько лет часто встречаются специальные хранилища секретов (а не только паролей, как раньше), известные как Vault. Возможность работы с ними стандарт в последней редакции не затронул, хотя во многих проектах такой способ используется повсеместно.

В то же время многие вендоры столкнулись с необходимостью доработки своих решений для соответствия ГОСТу в части способа хранения данных и необходимости накладывания шифрования.

Требования стандарта

В соответствии со стандартом система должна обеспечивать контроль предоставления, изменения или отзыва полномочий сотрудников для участников согласования. Это стоит учитывать при описании внедрения IdM, чтобы проект соответствовал ГОСТу.

> Значимый аспект, описанный в стандарте, – парольные политики, которые распространяются на автоматическое предоставление доступа.

Еще одна немаловажная процедура – контроль доступа через призму рисков, связанных с некоторыми полномочиями, ролями или информационными системами целиком. В новой редакции стандарта эта область носит рекомендательный характер, но изменения могут вноситься, поэтому всем производителям выдано предписание обеспечить наличие такой востребованной функциональности.

Один из участников ТК-362 предложил подход к регулярному пересмотру доступов сотрудников и подробному аудиту их данных и связанных с ними ролей и учетных записей. Изначально эта функция была востребована не везде, затем стала «золотым стандартом» и требованием согласно ряду приказов ФСТЭК (АУД, УПД, АН), а теперь еще является элементом ГОСТа. Не исключено, что некоторым разработчикам придется дополнительно потрудиться.

Обращает на себя внимание и пересмотр прав доступа при смене или добавлении трудоустройства. Как известно, один из производителей возвел это требование в стандартную процедуру в своем программном комплексе класса IdM. Единственный момент, который смутил многих заказчиков, – точное описание процесса регулярного пересмотра прав (так называемой сертификации). Должность «Руководитель ИБ» не подразумевает обязательного участия в согласовании.

В соответствии с документом решения класса IdM/IGA могут осуществлять обработку ПДн, поэтому при их внедрении необходимо рассматривать дополнительные меры и системы защиты информации.

Зная специфику и возможности этого класса решений, можно с большой вероятностью предположить, что новые редакции стандарта не за горами. ■