Многослойная защита: как уберечь ЦОД от вторжений

Игорь КИРИЛЛОВ

Когда говорят о безопасности ЦОД, чаще всего подразумевают защиту информационных активов. Но аспект физической охраны не менее важен, особенно в контексте коммерческих дата-центров, куда возможен доступ многих людей. Как же должна выглядеть идеальная оборона ЦОД, что об этом говорит мировая практика и какие решения используются в Украине?

Сегодня вопросам информационной безопасности внимания уделяется подчеркнуто много. Это, в общем-то, оправдано, особенно в контексте дата-центров. Ведь самое ценное в ЦОД — это данные и приложения, обеспечивающие предоставление услуг. Множество статей написано на тему того, как защитить свой комплекс от действий злонамеренных хакеров, взламывающих серверы и похищающих информацию. Действительно, это большая проблема. Но упускается из виду еще один немаловажный аспект — для современного дата-центра физическая составляющая безопасности важна не меньше, чем информационная. Иногда проще похитить сервер или жесткий диск, чем осуществлять удаленный взлом продвинутой системы информационной защиты. В экономически развитых странах, где рынок коммерческих дата-центров развит не в пример лучше украинского, такие случаи происходят не так уж редко. Правда, для Украины более актуальной является защита от внезапных действий силовых структур, но грамотно построенная система защиты поможет и в этом случае (о чем будет рассказано далее).

Хотя аспект физической безопасности актуален в равной степени для корпоративных и коммерческих дата-центров, во втором случае при прочих равных условиях эффективную систему защиты построить сложнее. Ведь в случае коммерческого ЦОД необходимо обеспечить удобный и своевременный доступ к оборудованию для большого числа клиентов, каждого из которых просто невозможно знать в лицо или проверить через внутреннюю службу безопасности. В то же время пользователь должен быть уверен, что его серверы и СХД находятся под надежной защитой и не могут попасть в руки посторонних лиц (в т.ч. самих сотрудников ЦОД). Как этого добиться? Ответ есть. Но для начала немного реальных историй.

Кевин Митник подобрался к дата-центрам

Статистика похищений ИТ-оборудования и физических взломов ЦОД не слишком обширна, поскольку большинство компаний предпочитают о ней умалчивать, маскируя инциденты с пропажей данных и остановкой сервисов под термином «технические неполадки». Поэтому скрыть не удается совсем уж вопиющие случаи, но и их за последние десять лет произошло немало. Так, в 2006 году из дата-

центра провайдера Level 3 (Лондон) было украдено несколько дорогостоящих плат маршрутизаторов операторского класса. Причем из действующего оборудования, что повлекло за собой серьезные сбои в работе компании и предоставлении услуг клиентам. Сложно понять, кому и для чего понадобились специализированные сетевые платы (возможно, это была диверсия со стороны конкурентов), но факт похищения скрыть не удалось.

В следующем году пострадал один из дата-центров крупнейшего телеком-оператора Verizon. В тот раз преступники, переодетые полицейскими, вошли в здание комплекса, нейтрализовали охрану и похитили оборудование стоимостью свыше $4 млн. В последующие несколько лет от «традиционных» налетов с использованием оружия пострадал еще не один ЦОД на территории США. Но самым большим неудачником в этом плане, очевидно, стоит признать коммерческий дата-центр C I Host, расположенный в Чикаго, который за два года четырежды подвергался разбойным нападениям и каждый раз успешно, несмотря на декларируемое внимание к системам безопасности.

Один случай был наиболее показательным. Тогда преступники проникли в здание комплекса с помощью пожарной лестницы, дождались, пока единственный охранник отлучился со своего поста, и устроили засаду. По возвращении последнего на него напали, обездвижили и связали. Затем, использовав личную магнитную карту жертвы и отпечаток пальца, злоумышленники проникли в машинный зал и похитили серверы одного из клиентов. Характерным в этой ситуации стало то, что единственное слабое звено — пункт охраны — стало причиной уязвимости в достаточно продуманной системе технических средств безопасности, включающих биометрическую идентификацию, видеонаблюдение, бронированные двери и т.д.

В 2011 году в одном из британских ЦОД компании Vodafone (г. Бейзинстоук) произошла кража сетевого оборудования и серверов. Сумма прямых убытков оказалась сравнительно небольшой, но в процессе кражи были серьезно повреждены операторские маршрутизаторы, что повлекло за собой серьезные сбои в работе сети мобильной связи длительностью в несколько часов и миллионные убытки (для компании такого класса средняя стоимость простоя составляет $9–10 тыс. в минуту). Да и персональные данные клиентов оказались под угрозой, что нанесло удар по репутации. В том же году похожий инцидент произошел и в ЦОД оператора O2.

Из числа более свежих происшествий можно упомянуть инциденты, произошедшие в 2015 году. Так, в Дании дата-центр интернет-провайдера Nianet был атакован преступниками, которые просто прорубили дыру во внешней стене, а затем вынесли серверы и другое ИТ-оборудование, а в Англии из дата-центра международной страховой группы RSA пропали накопители, содержащие важнейшую коммерческую информацию (включая персональные данные значительного числа клиентов банка Lloyds, в т.ч. имена, адреса и номера счетов).

Один из важных принципов безопасности гласит: «делай незаметным то, что защищаешь»

Совсем недавно, в апреле 2017 года, интерес к теме физической безопасности дата-центров подогрел знаменитый хакер Кевин Митник. В ходе своего выступления на ежегодной конференции Data Center World он детально рассказал о своем проникновении в коммерческий дата-центр, которое было осуществлено по заказу владельца комплекса, желающего проверить надежность физической защиты ЦОД. Как показал доклад, с помощью средств социальной инженерии и нехитрых технических приспособлений система безопасности, основанная на магнитных картах и электронных замках, была с легкостью преодолена.

Так что же это получается: если крупнейшие мировые операторы страдают от действий преступников, неужели у менее мощных компаний есть шанс устоять в случае целенаправленной атаки? Ответ здесь скорее «да», чем «нет», ведь во всех упомянутых случаях продуманная, на первый взгляд, система безопасности имела явное слабое звено. Почему так получилось — в каждом случае ответ будет своим, но как показывает опыт многих проектов, если оборона построена по всем правилам, то злоумышленникам ее не взломать. Что также подтверждено мировой практикой.

Эшелонированная оборона, или Принцип капусты

Хорошо спланированная и эффективная система физической безопасности дата-центра обычно включает в себя несколько последовательных ступеней — внешние уровни последовательно защищают внутренние зоны. Это главный принцип эшелонированной обороны. В логическом смысле такая схема чем-то напоминает кочан капусты, где внешние листья являются защитой и теплоизолятором для внутренних слоев. Причем в случае ЦОД каждый следующий уровень должен быть все более точным и персонифицированным. То есть если, скажем, в здание комплекса может проникнуть любой клиент, то к конкретной гермозоне или шкафу с оборудованием имеет доступ лишь конкретный проверенный человек. Немаловажно и то, чтобы правила контроля соблюдались как на входе, так и на выходе. Но обо всем по порядку.

«Нулевым» уровнем безопасности является сам выбор места размещения дата-центра, если, конечно, имеется такая возможность. Например, согласно стандарту TIA 942 Data Center Site Selection Criteria, ЦОД не должен располагаться в непосредственной близости от АЗС, аэропортов, рек, водохранилищ, военных баз,

Рис. 1. Охраняемый внешний периметр и въезд на территорию дата-центра T5 (Атланта, США)

складов с химическими материалами или ГСМ. К опасным объектам также относятся посольства и здания органов государственной власти.

Первым же настоящим препятствием для проникновения на территорию комплекса является внешний периметр безопасности, включающий забор (из бетона или прочных стальных прутьев) высотой не менее 3 метров, укрепленные въездные ворота (**рис. 1**), пункты физической охраны и система круглосуточного охранного видеонаблюдения, совмещенная с датчиками движения и средствами видеоаналитики.

Последний аспект является чрезвычайно важным, поскольку современные системы видеонаблюдения (СВН) без специализированного аналитического ПО лишаются большей части своих преимуществ. Человек-оператор не может эффективно следить за данными, получаемыми с большого количества камер наблюдения, тем более делать это круглосуточно. Не спасает положение даже работа в несколько смен. В то же время современные системы видеоаналитики могут определять подозрительную активность в кадре и сигнализировать о ней на пункт охраны.

Появление в запретной зоне «случайного» человека или машины не пройдет незамеченным. Также необходимо, чтобы камеры были оснащены антивандальной сигнализацией (сообщающей о повреждении устройства, расфокусировке или закрашивании объектива). Размещать их следует так, чтобы по периметру объекта не оставалось слепых зон. Ночью же для получения качественного изображения можно использовать мощную инфракрасную или лазерную подсветку. Камеры, расположенные на въездных воротах (как для посетителей, так и в зоне доставки оборудования) должны быть совмещены с ПО для распознавания автомобильных номеров. Но в любом случае решение о допуске человека или транспорта на территорию должен принимать дежурный охранник после проверки документов посетителей. Физическое ограничение доступа осуществляется с помощью турникетов (для людей), шлагбаумов и/или боллардов, выдвижных противотаранных столбов (для автомобилей) (**рис. 2**).

Рис. 2. Противотаранная система, установленная на въезде в один из американских ЦОД. Такое решение может остановить если не танк, то, по крайней мере, крупный грузовик

Нельзя забывать и о безопасности внешних объектов инженерной инфраструктуры ЦОД, которые, как правило, размещаются внутри внешнего периметра. Это холодильные машины, сухие градирни, ДГУ, электрические и кабельные вводы. Их также необходимо защищать с помощью антивандальных средств и по возможности сделать недосягаемыми для посетителей (оградив дополнительным забором, решетками и т.д.). Доступ к таким системам должен иметь лишь строго ограниченный круг сотрудников на основе электронных (лучше всего биометрических) средств аутентификации.

Кстати, оригинальный подход к охране периметра дата-центра продемонстрировала компания Google — ее ЦОД в округе Беркли (штат Калифорния, США) с прошлого года охраняет живой аллигатор. Дело в том, что комплекс окружен сетью искусственных водоемов, используемых для нужд системы охлаждения. Чтобы эти пруды не заиливались, в них развели популяцию специальных рыб, которые и привлекли рептилию. Новый сторож, длина которого сопоставима со средним человеческим ростом, сделал упомянутый дата-центр всемирно известным, чего, возможно, и не хотелось бы его владельцам, ведь еще один важный принцип безопасности гласит: «Делай незаметным то, что защищаешь».

Рис. 3. Полноростовый роторный турникет, совмещенный с СКД

Рис. 4. Шлюзовая кабина («стакан») на входе в помещение дата-центра

Идем дальше

Следующей зоной контроля является вход в здание и стойка регистрации («ресепшн»). Нередко, особенно в последние годы, дата-центры совмещают с бизнес-центрами. С одной стороны, это логично и удобно, но с другой — может создать дополнительные уязвимости в системе безопасности. Кевин Митник в упомянутом выше случае «взломал» именно такой дата-центр. В частности, он скопировал магнитную карточку одного из многочисленных офисных сотрудников и с ее помощью попал в здание.

Чтобы исключить такую возможность, за доступ в ЦОД должен отвечать отдельный пост охраны и собственные технические средства. В числе последних — бесконтактные считыватели магнитных карт, полноростовые турникеты (**рис. 3**) или даже шлюзовые кабины (**рис. 4**).

При этом в большинстве современных дата-центров магнитные карточки или специальные брелоки посетителей являются персональными, оформляются заранее и содержат всю важную информацию, включая фото. Таким образом, охранник или аналитическая система распознавания может визуально сравнить лицо входящего человека и настоящего владельца карты. Как видим, здесь тоже не обойтись без камер видеонаблюдения (вообще же СВН будет сопровождать нас на всех рассматриваемых этапах). Такой подход должен исключить возможность использования краденой карты и практику передачи пропуска третьим лицам. Надежным способом идентификации являются сканеры отпечатков пальцев, в том числе такие, которые позволяют определить пульсацию в кровеносных капиллярах пальцев (это исключает вероятность применения искусственного отпечатка), или детекторы, позволяющие определить посетителя по рисунку радужной оболочки глаза.

В некоторых случаях благодаря технологии Host-based Card Emulation ключом для доступа в здание дата-центра может стать обычный смартфон. Связь со считывателем в этом случае осуществляется с помощью технологии Near Field Communication, а пользовательский терминал играет роль виртуальной магнитной карты. Разработаны подобные решения и на базе Bluetooth. Одним из преимуществ такого метода является возможность динамического и практически моментального обновления или изменения криптографической информации ключей.

Но самым надежным подходом к организации доступа является, конечно же, многофакторная аутентификация, при которой пропускной пункт оснащен как считывателем магнитных карт, так и сканером отпечатков пальцев (такие устройства уже выпускаются в одном корпусе, иногда они дополнительно оснащаются еще и клавиатурой для ввода ПИН-кода) (**рис. 5**).

В некоторых случаях можно применять также биометрический считыватель черт лица (**рис. 6**). Такие решения уже доступны и на украинском рынке. Недостатком этих решений является то, что даже на сегодняшний день они все еще достаточно дороги. При этом физический пункт охраны также должен присутствовать — контроль со стороны живого охранника может осуществляться как на месте, так и удаленно с помощью средств СВН.

Рис. 5. Считыватель системы многофакторной аутентификации

Проблема налицо

Казалось бы, современные системы распознавания образов достигли значительных успехов. Человека можно идентифицировать не только по отпечаткам пальцев или сетчатке глаза, но и по лицу. Соответствующие сканеры используются во многих системах безопасности, в том числе и у нас в стране.

Тем не менее даже самые современные системы распознавания лиц, как оказалось, можно обойти, причем достаточно легко. Об этом свидетельствует недавнее исследование, проведенное учеными Университета Северной Каролины в Чепел-Хилл (США), результаты которого были обнародованы в начале 2017 года. Документ с деталями исследования под названием Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos имеется в открытом доступе. Перевести название можно примерно следующим образом: «Методы преодоления системы распознавания лиц с помощью виртуальной модели, составленной на основе фотографий человека, полученных из открытых источников», что в целом отражает суть проведенной работы.

В эксперименте участвовали два десятка добровольцев. На первом этапе их изображения были внесены в базы данных систем безопасности, использующих лицевые сканеры. Тестировались решения пяти различных производителей – 1U App, BioID, KeyLemon, Mobius, True Key.

Затем с помощью специального ПО на компьютере создавались 3-мерные мимические анимированные модели каждого добровольца. Материалом послужили личные фотографии. При этом в одном случае подопытных засняли на месте – в том же ракурсе и при том же освещении, как и в момент прохождения аутентификации. В другом случае работа велась только с фотографиями из открытых источников (в т.ч. социальных сетей). Текстура каждой 3-мерной модели имитировала человеческую кожу. Специальная программа воссоздавала сознательную и рефлекторную моторику лица, присущую живому человеку, осуществляла коррекцию взгляда и т.д. На заключительном этапе «оживленная» модель, работающая в режиме виртуальной реальности, выводилась на экран планшета и подносилась к сканеру. При этом изображение полностью имитировало движения головы и направление взгляда человека.

Результат оказался обескураживающим. Когда были использованы «идеальные» модели, заснятые в нужном ракурсе, все пять исследуемых систем были введены в заблуждение в 100% случаев. Во втором эксперименте, когда основой для модели служили фото из соцсетей, эффективность обмана несколько снизилась, но все равно осталась чрезвычайно высокой. Систему KeyLemon удалось обойти в 85% случаев, Mobius – 80%, True Key – 70%, BioID – 55% и лишь 1U App оказалась полностью взломоустойчивой. Но возможно, более совершенная 3-мерная модель позволила бы обойти и ее. В любом случае подобная статистика настораживает, особенно, учитывая тот факт, что аферу можно провернуть, используя вполне открытые данные. Другое следствие эксперимента заключается в том, что сканер лица сам по себе все еще не является достаточным средством аутентификации людей и должен применяться только в сочетании с другими элементами СКД.

Новые разработки в сфере идентификации посетителей поступают также из мира нанотехнологий. Временный электронный пропуск может печататься, например, в виде микроскопической схемы прямо на коже пальца, и такие разработки уже реализуются на практике. Правда, пока что их можно увидеть главным образом на крупных международных выставках, посвященных системам безопасности. Кстати, обзор современных технологий в сфере систем контроля доступа был опубликован в статье ***«Управляя доступом: новые тенденции на рынке СКУД», («СиБ» № 5, 2016***).

Рис. 6. Сканер лица может использоваться в качестве дополнительного фактора аутентификации посетителя

Все ближе к цели

Миновав пункт пропуска, контролирующий вход в здание, посетитель оказывается в непосредственной близости от машинного зала, и здесь также нужен повсеместный контроль. Камеры СВН надо располагать так, чтобы они позволяли видеть все коридоры и входы в помещения, а каждая дверь (в т.ч. в туалетах, лифтах) должна быть оборудована считывателем электронных карт либо биометрии (**рис. 7**).

Это необходимо для того, чтобы всегда иметь полную картину перемещения сотрудников и посетителей по внутренним помещениям и разграничивать права их доступа. Ведь на любом объекте есть комнаты, куда доступ клиентам запрещен, и наоборот — клиентское оборудование должно быть доступно только его владельцу (а в случае экстренной ситуации необходимо понимать, кто и какие действия совершал). Все это можно реализовать с помощью современных веб-ориентированных СКУД. Что касается камер видеонаблюдения, то в числе прочих требований они должны иметь возможность обеспечения достаточно качественного изображения в условиях аварийного освещения (если таковое предусмотрено). И, конечно же, все ключевые элементы системы безопасности — контроллеры управления, камеры, датчики, считыватели — должны быть подключены не только к основным, но и к запасным автономным источникам электропитания (например, ИБП).

Так или иначе, но попадая в помещение ЦОД, посетитель всегда должен быть под присмотром. В некоторых случаях, когда поток клиентов небольшой, каждого из них может сопровождать дежурный инженер.

Важным элементом внутренней системы контроля доступа являются средства сигнализации

Рис. 7. Любая дверь внутри дата-центра должна быть защищена с помощью элементов СКД

Рис. 8. Укрепленные двери, установленные на входах в машинные залы украинского ЦОД Gigacenter

и оповещения — уведомления об инцидентах или несанкционированном доступе должны направляться всем ответственным лицам. Не только на центральный пункт охраны дата-центра, но и руководству, например по SMS, электронной почте, другим каналам связи. Специальной зоной ответственности является центральный пункт охраны, в котором находятся средства управления системой контроля доступа и хранится архив видеозаписей с камер наблюдения. Доступ в это помещение должен регламентироваться особенно строго. Здесь не лишней будет упомянутая многофакторная идентификация. Отдельно требуется обеспечить физическую защиту ИТ-оборудования внутри самого помещения охраны. Серверы и СХД можно размещать в серверном шкафу, также оборудованном биометрическими считывателями, электромагнитными замками и охранной сигнализацией.

И, конечно же, сам вход в «святая святых» — машинный зал — также оборудуется средствами аутентификации пользователей. В дополнение к этому двери в это важнейшее помещение должны быть укрепленными (бронированными или даже пуле/взрывозащищенными) и пожароустойчивыми (**рис. 8**). Нельзя забывать и о качестве стен, прочность которых не должна уступать входным дверям.

Если они сделаны из железобетона — то этого вполне достаточно, но так бывает редко. Зачастую стена машинного зала представляет собой конструкцию из несущих колонн, пустоты между которыми заполнены газоблоками или кирпичами, а это не особенно надежное препятствие, которое достаточно легко преодолевается даже с помощью ручного инструмента. Кто будет долбить стену? Хороший вопрос. Но ведь ставятся же на входе в машинный зал противовзломные двери, значит, предполагается, что кто-то может попытаться их взломать. Так или иначе, но стены должны быть столь же трудным препятствием для злоумышленников, как и входные двери.

Самым надежным подходом к организации доступа является многофакторная аутентификация

Попав в машинный зал, посетитель также должен находиться под постоянным контролем (этой цели снова служит СВН) и получить возможность доступа лишь к собственному оборудованию. Для этого операторы дата-центров сооружают отдельные комнаты (гермозоны) внутри основного зала или отгораживают оборудование крупных клиентов прочными решетками (**рис. 9**).

Вход в такие зоны осуществляется с помощью обычного ключа, по электронным картам, брелокам либо с помощью дактилоскопического сканера. Нередко встречаются и обычные механические замки с особенным ключом. Защитить можно даже отдельную стойку. На рынке уже предлагаются серверные шкафы, оснащенные электрическими замками в сочетании с индивидуальными считывателями, в т.ч. использующими отпечаток пальца (**рис. 10**) в качестве ключа (хотя все же гораздо более распространены решения на базе электронных карт или обычных замков). В то же врем упомянутые отдельные элементы СКД можно установить самостоятельно даже на обычный серверный шкаф.

Последним рубежом обороны являются механические крепления ИТ-оборудования непосредственно в стойке или фиксаторы жестких дисков в серверах, которые, впрочем, обычно выполняются при помощи достаточно примитивных механических замков.

В коммерческих дата-центрах с общим зальным охлаждением особое внимание надо обратить также на фальшпол и вентиляционные шахты большого сечения. Существует потенциальная угроза, что злоумышленник, желающий получить доступ к оборудованию жертвы, может арендовать стойку или даже выделенную зону по соседству с интересующим его клиентом. Это позволит ему беспрепятственно попасть в машинный зал, а оттуда — в общее фальшпольное пространство. Высота подобной конструкции обычно не менее 800 мм, чего вполне достаточно для относительно свободного перемещения. Для исключения

Рис. 9. Выделенные зоны одного из клиентов внутри общего помещения коммерческого дата-центра

такой возможности клиентские модули нередко отгораживаются специальными вентилируемыми решетками, размещенными ниже уровня фальшпола.

Контроль, управление, учет

Но какие бы совершенные технические средства не применялись на объекте, сделать их по-настоящему эффективными можно только в составе единой системы. Это значит, что еще на этапе планирования должна быть разработана комплексная архитектура решения и определены основные риски, которые следует учесть. Важными элементами являются механизмы централизованного управления системой, возможность удаленного контроля и мониторинга, журналирование всех событий, настройка сигнализации и уведомлений. Необходима проработка протоколов действий сотрудников и клиентов, а также разграничение прав доступа к различному оборудованию и подсистемам дата-центра. Не менее важна и работа с персоналом, который необходимо подготовить для оперативного и адекватного реагирования на возможные угрозы.

Рис. 10. Серверная стойка, оснащенная электронным замком и дактилоскопическим сканером

Служба безопасности может быть как собственной, так и сторонней (коммерческой). Каждый подход имеет свои преимущества и недостатки, но оптимальным является их сочетание, поскольку ни одно охранное предприятие не готовит специалистов, знакомых со спецификой работы дата-центров. Лучше иметь в штате несколько постоянных работников службы безопасности, обученных действовать в условиях конкретного ЦОД. В случае же экстренной ситуации или срабатывания сигнализации следует уже вызывать сотрудников сторонней охранной организации.

Как защищены украинские ЦОД

Мы рассмотрели основные принципы построения систем физической безопасности в ЦОД. Но это опыт мировой практики. А какие средства и методы используют украинские операторы?

Система безопасности дата-центра компании ***BeMobile*** представляет собой достаточно сложный целостный комплекс, который соответствует требованиям стандарта TIA 942 Tier III и имеет сертификат соответствия ISO 27001 по безопасности.

Технически решение состоит из целого ряда взаимосвязанных подсистем (СВН, СКД, сигнализация), дополненных организационными процедурами, документами, инструкциями. Комплекс обеспечивает разграничение прав физического доступа как к оборудованию клиентов, так и к инженерной инфраструктуре дата-центра.

Здание ЦОД имеет три периметра охраны. Территория охраняется, доступ людям и транспорту органичен и осуществляется по предварительному согласованию. Пространство вокруг здания оснащено системой видеонаблюдения с инфракрасной подсветкой, без «слепых» зон, все изображения выводятся на экраны круглосуточного дежурного поста охраны (обеспечивается профессиональной охранной компанией) и диспетчерского центра ЦОД, где также всегда находятся несколько сотрудников, которые, кстати, не имеют права покинуть рабочее место одновременно. В ночное время, помимо видеонаблюдения, охрана осуществляет патрулирование периметра здания.

Доступ на территорию дата-центра осуществляется через специальный турникет и шлюз, пропускающий строго по одному человеку, при этом идентификация личности и права доступа посетителей регламентируются специальными процедурами. В их числе — оформление предварительных заявок и предъявление документов.

Внутри ЦОД каждый машинный зал (модуль) имеет собственную систему контроля доступа, поэтому сотрудник конкретного клиента во время посещения может попасть только в то помещение, в котором находится его оборудование, вся информация о перемещении посетителя фиксируется, записывается на электронных носителях и хранится два месяца.

В случае несанкционированного проникновения на территорию дата-центра срабатывает сигнализация и, в зависимости от ситуации, диспетчер принимает решение о вызове наряда ГСО при помощи «тревожной кнопки». Кроме того, каждый клиент имеет право устанавливать на свои модули дополнительные системы контроля доступа и видеонаблюдения. Каждая техническая система, обеспечивающая безопасность, продублирована либо может быть оперативно заменена в случае неполадок. Все процедуры доступа сотруд-

ников описываются в дополнениях к договорам, согласовываются со службами безопасности клиентов и самого дата-центра.

Дата-центр ***UnitedDC*** для обеспечения безопасности объекта также использует физическую охрану, СКД, подключение к пульту ГСО, охранные датчики, сигнализацию и СВН. В составе системы охранного видеонаблюдения более 80 цифровых камер с ИК-подсветкой — в т.ч. по шестнадцать в каждом из четырех машинных залов. При этом камеры, осуществляющие охрану внешнего периметра, имеют два контура безопасности — «предупреждения» и «тревоги». Видеоданные записываются и хранятся параллельно на двух СХД — локальной и удаленной.

На входе в дата-центр установлен специальный шлюз для ограничения группового прохода и возможности дополнительной проверки посетителей. Доступ на объект осуществляется с помощью электронных карт. Следующим пунктом является пост физической охраны, затем еще один рубеж пропуска на базе карт доступа и считывателей. После чего клиент попадает в закрытую зону, где его встречает дежурный сотрудник, который сопровождает посетителя в помещение ЦОД. Вход в машинный зал защищает противопожарная дверь толщиной 80 мм с биометрической системой доступа. Последняя способна распознавать не только отпечатки пальцев, но и лица клиентов. Межкоридорные двери обладают такими же параметрами, а также оснащены СКД на основе электронных карт (как на вход, так и на выход).

Внутри машинного зала клиентские шкафы и модули находятся под сигнализацией, доступ к ним осуществляется только в присутствии дежурного сотрудника после предварительного согласования времени проведения работ. Каждый модуль оснащен датчиками движения, затопления, задымления и др. Кроме того, в ряде случаев системами СКД и различными детекторами оборудуются даже отдельные клиентские шкафы.

Холодные коридоры во всех модулях дата-центра тоже закрыты на замок — ключи, как и журналы доступа, хранятся в специальных сейфах. Система безопасности постоянно мониторится, она объединена с общей шиной ModBus, которая, в свою очередь, подключена к единой периферийной шине дата-центра. История посещений контролируемых помещений дата-центра автоматически заносится в базу данных. Все процедуры безопасности, с учетом назначения ответственных сотрудников, четко регламентированы и прописаны в соответствующих внутренних документах.

В число основных средств безопасности ЦОД ***Gigacenter*** входит огражденный периметр вокруг отдельно стоящего здания, комплексная система круглосуточного видеонаблюдения, наружный пункт контроля (блокпост), два внутренних пункта физической охраны и подключение к пульту ГСО. Также имеется развитая внутренняя система СКД, позволяющая разграничивать права доступа в различные помещения дата-центра, установлены датчики движения и шлюзовая система доступа. Немаловажное значение играют отработанные регламенты безопасности, согласно которым любой сторонний человек не может находиться на территории дата-центра без сопровождения сотрудников оператора.

Прочность стен машинного зала не должна уступать прочности дверей

Система физической безопасности дата-центра «Парковый» обеспечивается с помощью целого ряда взаимосвязанных решений. Комплекс имеет два периметра физической безопасности. На внешнем расположены охраняемые контрольно-пропускные пункты, контролирующие которые доступ на внутреннюю территорию дата-центра. В самом ЦОД действует строгий пропускной режим (вход посетителей возможен только при наличии паспорта и в сопровождении сотрудника дата-центра). Все помещения оснащены датчиками движения, сигнализацией, магнитными замками, которые открываются исключительно личными бесконтактными RFID–браслетами. Вся информация поступает на главный пункт охраны. Кроме того, дата-центр подключен к пульту ГСО.

Видеонаблюдение построено на основе решения Cisco (Video Surveillance Operations Manager, камеры CIVS-IPC-6020 и CIVS-IPC-6030) и позволяет вести круглосуточный мониторинг происходящего в машинных залах и на территории комплекса. Для обеспечения доступа клиента к ИТ-оборудованию, предусмотрено программирование персональных RFID–браслетов, с их помощью посетитель получает доступ только в арендованные им помещения или блоки. Круг уполномоченных лиц, имеющих право доступа от имени клиента, оговаривается в дополнениях к договору и является его неотъемлемой частью.

Дата-центр ***«Воля»*** также защищен высоким забором с колючей проволокой и датчиками движения, внутренней СКД на базе электронных карт, системой видеонаблюдения. Последняя объединяет почти полсотни цифровых камер для охраны наружного и внутреннего периметров, машинных залов и т.д. Видеоархив хранится три месяца. Кроме того, объект подключен к пульту вызова охраны («тревожная кнопка»).

Чтобы попасть в ЦОД, посетителю нужно пройти авторизацию на контрольном посту и предоставить документ, удостоверяющий личность. Все данные о посещении вносятся в журнал, а клиенту выдается магнитная карта, которая необходима в дальнейшем для входа в само здание ЦОД. Попав в дата-центр, посетитель проходит еще одну авторизацию — в службе технической поддержки, где ему назначается уровень прав доступа к оборудованию: программный

(удаленное управление сервером), аппаратный (возможность физического доступа с системам) или даже разрешение на вынос того или иного оборудования. В любом случае доступ к оборудованию в серверной комнате предоставляется только в присутствии дежурного инженера технической поддержки. Входы в машинные залы защищают массивные взломоустойчивые двери: чтобы их открыть, нужно воспользоваться именной магнитной картой. При этом каждый сотрудник имеет свой уровень доступа в помещения, что контролируется централизованной СКД.

Этот список можно было бы продолжать, но нам бы пришлось многократно повторяться, ведь системы физической безопасности в различных украинских дата-центрах во многом схожи между собой. Поэтому мы упомянули лишь наиболее характерные примеры реализаций. В то же время, как показала практика, самой значительной угрозой для физической безопасности оборудования украинских дата-центров являются вовсе не уголовные элементы или злонамеренные действия конкурентов, а как раз те, кто должен был бы стоять на страже порядка.

Защита от защитников

За последние несколько лет отечественные ЦОД подверглись многочисленным атакам со стороны представителей силовых структур. Возможно, в ходе этих операций и были раскрыты какие-то преступления, но наряду с этим от непрофессиональных действия сотрудников государственных органов пострадало оборудование многих непричастных компаний, которым выпало несчастье разместить свои серверы в ЦОД, который по тем или иным причинам заинтересовал, скажем, Службу безопасности Украины.

Например, в апреле 2014 года представители СБУ и ГПУ проводили обыски в дата-центре «Парковый», при этом ИТ-оборудование было обесточено, что повлекло приостановку работы сервисов. В апреле 2015-го правоохранители нагрянули в харьковский коммерческий ЦОД StepHost, где конфисковали 130 серверов, а менее чем через год от обысков силовых структур пострадал киевский дата-центр «Адамант». При этом во всех случаях поводы были надуманными (что подтверждается отсутствием приговоров суда), но многие клиенты пострадали. В то же время не зарегистрировано ни одного инцидента, нарушившего работу оборудования украинского ЦОД, связанного с действиями преступников. Так что имеющиеся системы безопасности дата-центров довольно хорошо защищают их от злоумышленников. Но можно ли уберечься от неправомерных действий силовых структур? В теории — да, но на практике это стоит больших усилий без гарантии успеха.

Попадая в помещение ЦОД, посетитель всегда должен быть под присмотром

Как сообщают представители некоторых дата-центров, общая линия обороны может выстраиваться следующим образом. Во-первых, необходимо, чтобы средства контроля доступа были действительно труднопреодолимыми: мощные болларды или другие заграждения, препятствующие проезду автотранспорта, толстые бронированные двери, полноростовые турникеты из прочной стали и т.д. Во-вторых, у дежурного на пункте охраны должна быть возможность экстренной блокировки упомянутых систем, чтобы обратную разблокировку физически мог осуществить только представитель руководства с помощью специальных ключей. Это лишит нападающих преимущества от эффекта неожиданности. В то же время, чтобы не подвергать потенциальной опасности людей, находящихся в помещении ЦОД, также должен быть предусмотрен механизм безусловной принудительной разблокировки выходов, но включаться он должен только в случае срабатывания пожарной сигнализации.

Вскрытие мощных охранных конструкций в любом случае — достаточно длительный процесс. За это время сотрудников силовых структур должно встретить руководство комплекса и, главное, представители юридического отдела, которые проверят правомерность претензий. К тому же о ситуации необходимо уведомить клиентов, которые могут начать резервное копирование данных и переход на запасные площадки с целью минимизации потенциального ущерба.

Параллельно с этим по всем доступным каналам коммуникаций надо оперативно распространять информацию об инциденте — привлекая внимание общественности и прессы (благо развитие социальных сетей позволяет распространять информацию практически моментально среди широкого круга людей). Эту часть — куда писать, кому звонить — лучше предусмотреть и отработать заранее, ее выполнением может заняться, например, ПР-отдел. Сочетание трех факторов: лишение эффекта неожиданности, юридический надзор и придание гласности способно если не отвратить атаку, то, во всяком случае, максимально удержать ее в рамках правового поля, чего во многих случаях было бы достаточно для того, чтобы в ходе спецоперации не пострадали непричастные клиенты.

Как показывает практика, несмотря на отдельные инциденты, системы безопасности современных дата-центров достаточно эффективно справляются со своими задачами. Явных «проколов» все же немного. Но по мере усиления роли ИТ в повседневной жизни растет и цена ошибки, а значит, охранные системы и процедуры будут совершенствоваться. В то же время хочется, чтобы в Украине защищать дата-центры впредь надо было бы только от преступников, а не от тех, кто по задумке должен с ними бороться.

Игорь КИРИЛЛОВ, СиБ