

КОЛОНКА РЕДАКТОРА

Учет рабочего времени
в торговых сетях

Розничная торговля в России развивается стремительными темпами. Крупные торговые розничные предприятия представлены во многих регионах России в виде сетей из множества отдель-

ных гипермаркетов, супермаркетов, а также торговых организаций вида "магазин-за углом". Некоторые крупные сети включают в себя более тысячи магазинов, в которых работают десятки тысяч людей. Существует множество важнейших задач для таких предприятий, в том числе в сфере безопасности, от решения которых зависит эффективность работы и финансовые показатели торговой сети. Степень важности этих задач зависит от масштаба торгового предприятия, от его специализации и других факторов.

Важнейшими задачами в сфере безопасности для торговых розничных сетей являются:

- 1) учет рабочего времени сотрудников;
- 2) разработка и внедрение на предприятиях программ лояльности;
- 3) контроль доступа в складских и торговых помещениях;
- 4) автоматизация сбора данных, отчетность.

Для крупных торговых сетей среди этих задач, возможно, наиболее важной является учет рабочего времени сотрудников. В отличие от других предприятий в крупных сетях много сотрудников имеют сменное, индивидуальное расписание. Для учета рабочего времени сотрудников с различными графиками работ в последнее время приобретают популярность биометрические терминалы по отпечаткам пальцев и по карте. Терминалы учета рабочего времени устанавливаются в каждом магазине торговой сети. Для этих предприятий разрабатывается территориально распределенная информационная система, в которой отображается список всех магазинов, установленных на них терминалов с возможностью получить состояние каждого из этих устройств, добавить сотрудника, получить отчетность по тому или иному магазину, получить список опоздавших или отсутствующих на работе сотрудников и другие данные. В головном офисе, как правило, выделяются некоторые серверы для поддержки данной системы и администратор для обслуживания данной системы.

Шамиль Оцоков

Редактор рубрики
"Управление идентификацией",
руководитель разработки
программного обеспечения
компании "Сонда Эксперт", д.т.н.

Человеческий фактор в системе контроля и управления доступом

Человеческий фактор пользователей, который мешает работать замечательной спроектированной системе контроля и управления доступом – это как зима, которая в сотый раз настала неожиданно и почему-то снова со снегом



Алексей Омельянчук
Начальник КБ "Рубикон"
ГК "Сигма"

Думаете, я сейчас буду рассказывать страшилки про мерзких пользователей, которые не понимают своего счастья и ломают замечательныеСКУД? Таких историй у меня много. И про солдат-срочников, которые быстро обнаруживают, что при подборе кода реже чем 1 раз в 30 секунд тревоги не будет и потому подбирают 4-значный код всего за пару дежурств. И про секретаршу, которой лень оформлять посетителю пропуск и потому она его пропускает через грузовые ворота, которые потом стоят приоткрытые полдня. Или хотя бы про самый распространенный вариант – на двери комнаты считыватель, а дверь стоит открытой и подпертой кирпичом. Да, это все человеческий фактор. Но виноваты не пользователи.

Контроль доступа "для красоты"

Начнем в обратном порядке. Дверь подперта кирпичом, потому что иначе в комнате душно. Проблема – в плохой системе вентиляции. А в результатеСКУД что есть, что нет – для красоты лампочки помаргивают.

Секретарше лень оформить пропуск. А кому будет не лень, если для этого надо пешком сбежать в соседний корпус с бумажной заявкой. Что? Web-интерфейс, распределенные системы? Нет, не слышали... Ну и что начальство хочет? Разве секретарша только и мечтает защищать имущество или какие-нибудь госсекреты? Чего от нее ждут?

Солдат-срочник на посту от нечего делать подбирает код на цифровом замке? А чем ему еще заниматься? Попробуйте ничего не делать сутки в наряде, на 10-й раз начнете открывать ног-

тем замок, а на 12-й на одной двери открутите магнитик и на всех остальных найдете, где такие магнетики стоят с другой стороны, вскрывай – не хочу. Говорят, его туда поставили все это охранять, а не ломать? Если бы верили, что он это будет охранять, то проСКУД бы и речи не было, он бы и охранял. На самом-то деле понятно, чтоСКУД именно от него будет защищать все то, что внутри. Так и следует планировать защиту от человека с бесконечным количеством свободного времени. Этот демобилизуется, другому передаст, на чем остановился, следующий будет продолжать перебирать циферки. Год – и 6-значный код подобран. Хорошо, не год, а два – ведь иногда надо изображать бдительное несение службы, вдруг майора принесет.

За пределами фантастики

Еще раз и медленно: главная проблема плохо работающих системСКУД – это человеческий фактор. В основном – на этапе проектированияСКУД или смежных систем.

Особенно меня радуют вошедшие в моду последние лет 10 "комплексные концепции работыСКУД", которые составляют специально нанятые эксперты для особо серьезных объектов. В большинстве случаев это жуткая комбинация из голливудской фантастики и желаний супергермского ограничить доступ плюс иногда неудачные попытки переложить на терминыСКУД проверенные временем принципы организационных мер.

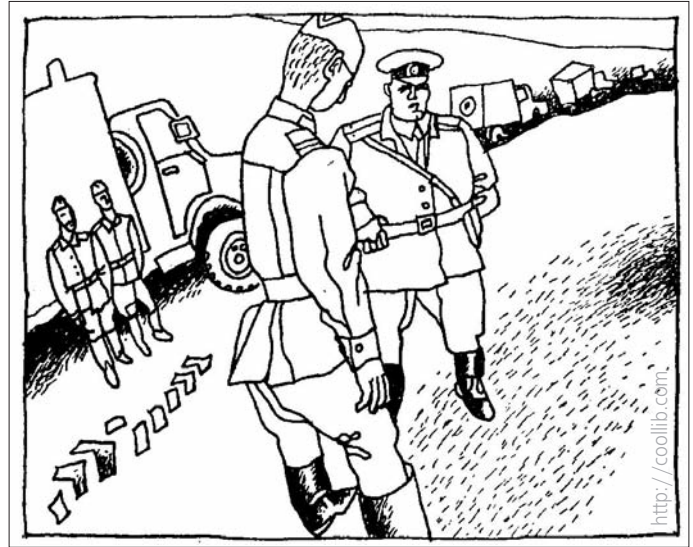
Как пример – "принцип комиссионности", когда доступ в помещение, например, с ядерной бомбой или золотом республики предоставляется только при наличии трех разных ключей трех разных людей – командир, комиссар и бортинженер. Изначально все разумно, но только если это требуется именно для первичного вскрытия стоящей на охране комнаты. Мы это делали, это работает. А если потребовать три карты для каждого открывания двери, и после некоторого количества открываний один вошел, а два остальных задержались снаружи, то что им теперь делать? Звать по мобильнику из отпуска запасного третьего? Так там еще и глушилки мобильной связи стоят...

Обыкновенная реальность

В большинстве случаев фантастика в техзаданиях мягко игнорируется на стадии пусконаладки. Демонстрируется принципиальная возможность настроить, например, жесточайший контроль повторного прохода, дальше пишется запрос к службе безопасности, на какие зоны



Web-интерфейс, распределенные системы? Нет, не слышали...



Попробуйте ничего не делать сутки в наряде, на 10-й раз начнете открывать ногтем замок

контроля разбить объект, и поскольку никто на этот запрос не отвечает, то и никакой "жесткий Antipassback!" никто не настраивает.

Благо, реальные люди, занимающиеся реальной безопасностью, а не "эксперты", приглашенные проявить свою фантазию, предпочитают начинать с простых режимов и лишь потом по возможности что-то усиливают чем-то особенным. Но иногда из-за необходимости удовлетворить техзадание на этапе конкурса в проект изначально закладываются, скажем, полноростовые турникеты в переходах из корпуса в корпус. А то иначе тот самый Antipassback будет постоянно нарушаться – карту предъявил один, а прошли в дверь пятеро...

А теперь вспомним, что через этот коридор зимой все будут не только ходить, но и грузы таскать, ибо на улице -40 °С, и внешняя дверь во второй корпус будет напрочь забита для теплоизоляции. И сколько там простоит этот турникет? Отвинтят и отставят в сторону, чтобы не мешался. И не надо валить на человеческий фактор пользователей. То есть я хотел сказать – "неча на зеркало пенять"...

Много проблем – одно решение

Современные СКУД изначально были придуманы и развивались именно для того, чтобы максимально учитывать человеческий фактор. Можно (и это местами делалось) заставить всех штатных сотрудников организации отпирать дверь своим ключом и захлопывать ее за собой – чтобы все двери всегда были закрыты и никто посторонний не мог случайно зайти в пустой кабинет с секретными штабными картами. Это ужасно трудно реализовать. Только если сотрудники действительно отлично понимают важность секретности и в соответствии с ней получают жалование.



А если пользователи – это милые дети...

СКУД позволяют за сопоставимую с ценой обычного хорошего замка сумму обеспечить ситуацию, когда двери действительно будут постоянно закрыты, а сотрудники будут ходить, помахивая карточками и проходя в эти двери, не задерживаясь вместе с кипами очень важных бумаг под мышкой. И это не в генеральском штабе, а даже в самом расплоднем МРЭО, где стройные сотрудницы в поте лица таскают тяжеленные пакки номерных знаков.

И как мелкий бонус можно тонко разграничить, кто куда может ходить, но это уже малое добавление. Главное, что двери, наконец, закрыты почти всегда по сравнению с постоянно открытыми, как было раньше (и как снова будет, если неумеренными фантазиями опять создать проблемы персоналу).

Все гениальное просто

Если пользователи – сотрудники атомной электростанции, отлично понимающие опасность того, что внутри, и тщательно выполняющие

инструкции с переодеваниями (и получающие соответствующий регулярный инструктаж и соответствующую регулярную зарплату), можно ожидать, что они спокойно и точно выполнят процедуры проходов через шлюзы на КПП и через пару турникетов с жестким контролем прохода уже в реакторных корпусах. Тем более, они знают, что жесткий учет "Кто находится внутри" нужен в первую очередь для того, чтобы в случае любой аварии знать, кого откуда спасать.

А если пользователи – это милые дети... Помнится, самые бронебойные вандалостойкие кожухи для видеокамер у фирмы Philips (когда она еще занималась выпуском камер видеонаблюдения) были в разделе "Для тюрем и школ".

Думаете, это только голландские школьники ведут себя так же, как закоренелые бандиты? Сейчас во многих школах в Москве на входе поставили турникеты, и можно увидеть, как полтысячи милых деток штурмуют этот турникет в последние 10 минут перед звонком... Снизу, сверху, сбоку, втроем (!) по одной карте... И охранник, который с привычным ворчанием открывает калитку и пускает всех мимо, когда кто-то опять намотался на турникет шнурками от ботинок так, что его оттуда полчаса разматывать, и все заклинило... Я, конечно, сгущаю краски, я все это видел, но не одновременно, не в одно утро, а в разные дни. Но турникет, заклинивший из-за намотанных на него кроссовок, – был. Сам "милый дет" при этом, видимо босиком, успешно убежал на уроки.

Хотите увидеть самый опасный для СКУД человеческий фактор? Сейчас это доступно каждому. Берете свой телефон, включаете режим "Фото" и переключаете на переднюю камеру. Всматриваетесь в лицо этого человека и говорите ему: "Будь проще, не морочь голову себе и людям".

¹ Антипассбэк (англ. Antipassback) – защита от передачи пропуска назад следующему входящему. В наиболее строгом варианте означает постоянное отслеживание последнего места применения карты-пропуска, при этом если человек не вошел легально, например, в коридор 2 этажа, то в доступе в любую комнату 2 этажа ему будет отказано.

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru