

СКУД, трудовая дисциплина и безопасность на объекте

Леонид МЕДВЕДЕВ, преподаватель учебного центра «Информзащита»



Что же объединяет эти три понятия? СКУД и безопасность — тут вроде бы все ясно. Система контроля и управления доступом — это часть системы объектовой безопасности, все более активно внедряемая на предприятиях. Как трудовая дисциплина должна быть связана со СКУД, вроде тоже понятно: зашел сотрудник на территорию, провел HID-картой по считывающему устройству, и в логе системы сохранилась информация о дате и времени прихода на работу человека. Вышел сотрудник за территорию предприятия, воспользовался картой для разблокировки двери — в логе опять запись о времени ухода. СКУД — довольно удобный инструмент кадрового контроля, и многие предприятия этим пользуются. К сожалению, практика показывает, что возможности кадрового контроля чаще всего используются в минимальном объеме, а о том, что эффективно использующаяся система контроля управления доступом может решать очень широкий спектр вопросов — как кадровых, так и касающихся работы всей системы безопасности предприятия, включая систему охраны труда, — многие почему-то забывают.

Поводом для написания этой статьи стал несчастный случай на производстве, который мне как приглашенному эксперту пришлось расследовать. Предпосылками происшествия стали несоблюдение трудовой дисциплины, нарушение правил техники безопасности на производстве, ошибка в алгоритме СКУД и напрямую связанные с этой ошибкой действия, а точнее, бездействие службы охраны. Суть происшествия довольно проста. Сотрудник компании ХХХ Иванов в рабочее время зашел на производственную территорию, куда формально не имел допуска, и, будучи не ознакомлен с правилами техники безопасности, получил травму от работающего механизма. Подобные происшествия случаются довольно часто, и, как правило, для их разбора не возникает необходимости приглашать эксперта со стороны. В данном же случае основанием для серьезного расследования инцидента стала недавно установленная на предприятии система СКУД. То есть по логике заказчиков этой системы данный сотрудник, не имея допуска, не мог сам попасть на производственную территорию. Не мог, не должен был, а попал.

Результаты расследования показали, что причина происшествия вполне банальная и, к сожалению, довольно распространенная. Пострадавший сотрудник зашел на производственную территорию вместе с работающим там сотрудником Петровым, воспользовавшись тем, что сотрудник Петров разблокировал дверь на производственную территорию своим электронным пропуском (HID-картой). Сотрудник Петров не обратил внимания на то, что с ним на территорию зашел посторонний, так как дело происходило на огороженной охраняемой территории предприятия ХХХ, и, по мнению сотрудника Петрова, посторонних на территории предприятия быть не могло.

Теперь давайте абстрагируемся от этого происшествия и вспомним, сколько раз мы с вами наблюдали картину, когда на территории предприятия, оснащенной системой СКУД, несколько сотрудников проходят в дверь, оборудованную системой контроля доступа по

HID-карте одного из них. То есть один карточку приложил — 10 человек зашли. Включите в эту группу трех посторонних людей, у которых вообще нет никакого права доступа, и они прекрасно пройдут с группой сотрудников, и с вероятностью 98% никто из группы не заинтересуется, кто это и куда идет. Раз оказался на охраняемой территории, значит, ему можно, раз идет, значит, ему нужно. Точно таким же способом на охраняемую территорию одной весьма известной западной компании проникли злоумышленники, которые, украв личные вещи, деньги и т. п. у сотрудников этой компании, аналогичным образом покинули охраняемую территорию, напичканную системами контроля и ограничения доступа. И подобных случаев, к сожалению, немало.

Проводя аудиты объектовой безопасности, мне часто приходится видеть, что хорошая, дорогая система управления доступом используется с эффективностью 10–15%. То есть она работает на уровне обычного кодового замка. Зачем же идти на такие траты, если кодовые замки стоят на несколько порядков дешевле? И если деньги на дорогостоящую СКУД уже потрачены, система установлена и работает, почему бы не использовать ее более эффективно? Чаще всего причина неэффективного использования уже имеющегося и работающего оборудования на удивление банальна. Задействуя весь функционал СКУД, мы тем самым увеличиваем нагрузку на сотрудников службы безопасности. При этом увеличивается именно нагрузка на существующих сотрудников без необходимости увеличивать штат. И сотрудники охраны, часто негласно поддерживаемые в этом своим непосредственным руководством, начинают всячески саботировать работу СКУД, отключая те или иные функции. Ведь им вместо спокойного сидения на теплом месте за чашкой чая или книжкой приходится много бегать и много работать.

Следующая по распространенности причина неэффективного использования СКУД — экономия. Предприятие закупает дорогостоящий комплекс, но экономит на отдельных его элементах и располагает преграждающие устройства, устройства контроля, устройство контроля состояния преград только в местах входа сотрудников на территорию, а про различное вспомогательное оборудование вообще речи не идет. Получается, что установленная система СКУД просто дублирует вахтера на входе в здание. И говорить здесь о каком-либо кадровом контроле, как правило, не приходится. Наглядным примером такого подхода является ситуация, когда гостевой пропуск выписывает вахтер на входе, заносит данные посетителя в журнал учета и выдавая универсальную, заранее прошитую HID-карту, к записи в журнале посещений не привязанную. Электронная карта вроде бы есть, но она безлика и не позволяет контролировать перемещения конкретного посетителя. А ведь HID расшифровывается как карта идентификации человека. То есть мы опять возвращаемся к обычному кодовому замку, пусть и очень дорогому.



Третья по распространенности причина неэффективного использования систем СКУД — незнание возможностей системы и неумение этими возможностями пользоваться. Предприятие заказывает разработку и монтаж дорогостоящей системы и при этом экономит, по сути, копейки на обучении персонала, который на этой системе должен работать. В результате мы опять имеем дорогостоящую систему, работающую с эффективностью примитивного кодового замка.

Ну и последняя, на мой взгляд, наиболее редко встречающаяся причина неэффективной работы СКУД — это ошибки в алгоритмах, возникающие, как правило, из-за неверно сформулированных задач. То есть, по сути, из-за некомпетентности заказчика.

Давайте опять вернемся к несчастному случаю в компании ХХХ. Да, его причиной стал несанкционированный проход сотрудника компании на территорию с ограниченным доступом. То есть налицо явное нарушение трудовой дисциплины. Но возможным это стало из-за того, что система контроля, позволяющая выявлять подобные случаи, была отключена сотрудниками службы охраны, которым не хотелось лишний раз отрываться от теплого места и куда-то бежать. Говоря человеческим языком, сотрудники службы охраны были практически беспомощными в подобных ситуациях из-за отсутствия каких-либо способов воздействия на нарушителя, кроме возможности взять его за руку и вывести с запретной территории. Ни штрафов, ни каких-либо служебных взысканий для сотрудников за подобные нарушения в компании ХХХ предусмотрено не было.

Практика же показывает, что делать бессмысленную работу никто не любит и, если сотрудник видит, что его действия не приносят результата, он очень быстро начинает относиться к выполнению своих служебных обязанностей спустя рукава.

Мне довольно часто приходилось слышать аргументы, в том числе от руководителей служб безопасности предприятий, что контроль за соблюдением всех требований системы управления доступом существенно увеличивает нагрузку на сотрудников службы охраны, которым это не нравится, а так как зарплаты у них чаще всего небольшие, это становится проблемой. Но есть одна тонкость. При наличии действенных механизмов не только контроля, но и воздействия на нарушителей нагрузка на службу

охраны существенно увеличивается только на период становления системы. Два-три штрафа, наложенные на любителей использовать для прохода одну HID-карту на группу сотрудников (при этом штрафовать должны все уклонившиеся от идентификации), широкое освещение этих случаев среди сотрудников предприятия — и все дисциплинированно начинают идентифицироваться при проходе через средства контроля. Мой опыт построения охранных систем и организации служб охраны объектов говорит, что организационный период, даже на крупном предприятии, при правильно построенных алгоритмах охранной деятельности и кадрового контроля редко продолжается больше одного-двух месяцев. Если же за каждый случай выявления уклонения от идентификации либо любого другого нарушения правил поведения на объекте премировать дежурную смену охраны, подобные инциденты сходят на нет очень быстро.

В заключение хочу сказать, что знаю довольно много предприятий, на которых система контроля и управления доступом функционирует в полном объеме. Статистика говорит, что на таких предприятиях производительность труда в два раза выше, нежели в компаниях, где СКУД не используется. Ведь система контролирует не только допуск сотрудников, но и учитывает время прихода на работу и ухода домой, время, потраченное на обед, время, потраченное на перекуры, время на рабочем месте и время хождения по территории. Руководство компаний после запуска системы СКУД часто с удивлением выясняет, что в среднем КПД работников компании редко превышает 30%. Задействование же механизмов кадрового контроля очень быстро позволяет увеличить этот показатель до 70–80%, что, в свою очередь, не может не сказаться на благополучии предприятия. ☑

ГРАДОХРАНИТЕЛЬ

СИСТЕМА МОНИТОРИНГА ОПАСНЫХ СИТУАЦИЙ

Прибор "Хранитель-IT"

Выполняет свои функции по контролю опасных ситуаций и локальному оповещению при их возникновении, полностью автономно. Принципиально важной особенностью прибора является использование новейших «облачных» IT-технологий для обмена информацией между прибором и пользователем через единый центр обработки данных (ЦОД), находящийся удаленно от прибора.



ПУЛЬТ ЭКСТРЕННОЙ ПОМОЩИ

- ЧОП
- полиция
- МЧС
- скорая помощь

ИНТЕРНЕТ-ПРОВАЙДЕР

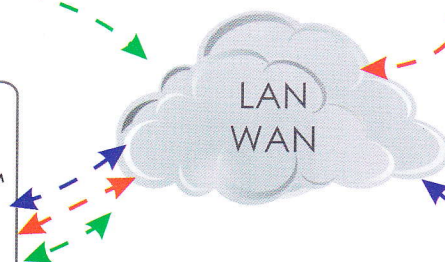
- предоставление услуги "Мониторинг ОС"
- поддержка аккаунта пользователя
- биллинг

КЛИЕНТСКАЯ ЗОНА

- Wi-Fi
- Ethernet

ДАТА-ЦЕНТР "Хранитель"

- ведение базы данных
- выдача данных пользователям
- управление пультами
- диагностика системы
- техническая поддержка



УДАЛЁННОЕ УПРАВЛЕНИЕ С МОБИЛЬНЫХ УСТРОЙСТВ ПОД ОС "Андроид"

- оповещение об опасных ситуациях в жилище
- полная информация о текущем состоянии системы
- запрос архивных данных
- отправка сигнала SOS домой и прием из дома
- дистанционное управление прибором