Проблемы использования видеонаблюдения в компании

Игорь СОБЕЦКИЙ,
заведующий кафедрой экономической безопасности учебного центра «Информзащита»

Ищут пожарные,
Ищет милиция,
Ищут фотографы
В нашей столице,
Ищут давно,
Но не могут найти
Парня какого-то
Лет двадцати.

Попытка идентификации нарушителя по видеозаписи

Видеонаблюдение в российских компаниях стало уже не столько одним из аспектов безопасности, сколько модным аксессуаром. Видеокамеры работают даже в ларьках, не говоря уже о сколько-нибудь заметных компаниях. Однако далеко не все руководители готовы вкладывать в систему видеонаблюдения значительные средства. Стоит только всерьез приступить к организации видеонаблюдения, как неожиданно выясняется, что эффективная система и услуги специалистов в этом вопросе стоят весьма существенных денег. В результате после трезвого анализа рыночных цен делается выбор в пользу наиболее экономичных вариантов.

На самом деле еще до написания технического задания на систему видеонаблюдения (не говоря о проекте) необходимо решить, для чего будет использоваться видеонаблюдение в компании. Как правило, используется один из двух вариантов:

• оперативное видеонаблюдение — система рассчитана на контроль обстановки в компании в реальном времени и немедленное реагирование на выявленные инциденты;

• архивное видеонаблюдение — система рассчитана на постоянное документирование обстановки в компании с целью обеспечения последующего расследования инцидентов безопасности и получения материалов, позволяющих выявить нарушителей.

В первом варианте допустимо использование относительно дешевых и низкокачественных аналоговых камер и низкоскоростных линий передачи видеосигнала. Видеорегистратор, если он есть, используется преимущественно для контроля технической исправности камер. Основные расходы в этом варианте приходятся на оборудование помещения для операторов наблюдения, обеспечение их круглосуточной работы и организацию постоянно действующих оперативных групп службы безопасности, готовых к немедленной локализации выявленных операторами инцидентов. Расходы на персонал значительно превышают расходы на оборудование, причем носят постоянный характер.

Во втором варианте на персонале можно сэкономить. Каких-то специально выделенных работников не потребуется, а просмотр и анализ записей в случае необходимости способен выполнить любой работник службы безопасности компании. Зато предстоит потратиться на высококачественные управляемые камеры, высокоскоростные линии передачи данных и мощную систему хранения данных с соответствующим программным обеспечением. Первичные затраты существенно выше, чем в первом варианте, зато эксплуатационные расходы минимальны.

Однако эта логика, как уже говорилось, живет до первого знакомства с действующими ценами. Выясняется, что аналоговая купольная камера может стоить в 10–15 раз дешевле управляемой цифровой.

Цены на видеорегистраторы отличаются еще больше. Если недорогой аналоговый регистратор — тот самый, который применяется для контроля камер в системе оперативного видеонаблюдения, — обойдется в 10 000–20 000 руб., то за серьезную систему хранения

цифровых видеоданных придется заплатить около миллиона. Не мудрено, что в некоторых компаниях специалистов, агитирующих за создание системы архивного видеонаблюдения, всерьез обвиняют в получении откатов!

Поскольку на дворе кризис, генеральный директор – и в некоторых случаях специалист по безопасности – выбирает самое экономное решение. Корпоративное видеонаблюдение строится по типу архивного на комплектующих для оперативного. Получается дешевый, понятный акционерам и руководству и, в принципе, как-то работающий вариант.

Единственное неудобство: данный вариант годится лишь для успокоения руководящих нервов и вселения страха в сердце потенциальных нарушителей. Если же случается реальный инцидент, то идентифицировать нарушителя оказывается непросто – примеры показаны ниже.

К сожалению, обычно эта проблема всплывает только после того, как бюджетная система видеонаблюдения уже смонтирована. Приходится вспоминать скупого, который платит дважды, и переделывать систему с нуля[1].

Вторая проблема, вставшая перед службой безопасности[2], – насколько законно видеонаблюдение на объектах компании. Остерегаясь судебного преследования со стороны поборников прав человека, некоторые специалисты отказываются от идеи использовать в компании эффективные системы видеонаблюдения. Рассмотрим ситуацию более подробно.

Очевидно, что, в принципе, нарушать чьи-либо права может лишь видеозапись, содержащая идентифицирующую информацию, т. е. позволяющая однозначно установить запечатленных на ней лиц. Видеоролик, содержащий смазанное изображение силуэта, форсирующего дыру в заборе, ничьих прав ущемлять не может, если, конечно, не сопровождается субтитрами. Поэтому из конфликтного поля сразу же выпадают все системы оперативного видеонаблюдения. Законность же систем архивного видеонаблюдения доказывается легко. Использование систем видеонаблюдения в Российской Федерации не противоречит действующему законодательству и никак не нарушает прав на неприкосновенность личности. Некоторые юристы ссылаются на Конституцию РФ:

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Однако в той же Конституции РФ прямо говорится, что права одного человека не абсолютны:

Статья 17

1. В Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права и в соответствии с настоящей Конституцией.

2. Основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения.

3. Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц.

Таким образом, осуществление прав и свобод работника не должно нарушать права и свободы работодателя, в том числе права на сохранность своего имущества. Территория предприятия является таким же общественным местом, как, например, городская улица. Поэтому работодатель вправе осуществлять здесь видеонаблюдение. Конечно, о системе видеонаблюдения на объекте работодатель должен уведомить как персонал, так и посетителей, разместив соответствующие таблички. Вопреки мнению ряда юристов автор не считает необходимым получение согласия работников или других лиц на видеонаблюдение. При наличии предупреждающих табличек это согласие выражается конклюдентными действиями – если работник прошел в здание, он согласен на видеонаблюдение.

Всё изложенное справедливо лишь для открыто установленной системы видеонаблюдения – с видимыми камерами и предупреждающими табличками. Установка скрытых видеокамер без табличек, по сути, как раз и является «подпольной» оперативно-розыскной деятельностью. Скрытые камеры в таком случае могут быть признаны специальным техническим средством для негласного получения информации. Кроме того, даже на предприятии есть помещения, где неприкосновенность частной жизни охраняется законом, – туалеты, раздевалки и душевые кабины. Установка в этих помещениях каких-либо видеокамер будет существенным нарушением прав работников.

Право работодателя на использование систем видеонаблюдения не ограничено также законом № 152-ФЗ «О персональных данных». Разумеется, видеозапись вполне можно рассматривать как биометрические персональные данные. По этому поводу в законе, в частности, говорится:

Статья 11. БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством

[1] Автору известен случай, когда при использовании такой бюджетной системы в целях добиться хоть какого-то результата на спецовках рабочих склада были крупно написаны номера. Такой подход привел к многочисленным конфликтам на предприятии.

[2] Обычно с подачи корпоративного юрисконсульта.

Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Таким образом, закон, не исключая вообще факта обработки биометрических персональных данных, накладывает особые условия их обработки (письменное согласие субъекта) только в одном конкретном случае: когда целью обработки биометрических данных является установление личности субъекта. В остальных случаях ограничения на обработку биометрических данных закон не предусматривает. То есть основным квалифицирующим признаком отнесения системы видеонаблюдения под статью 11 закона № 152-ФЗ будет являться не сам факт обработки биометрических персональных данных, а факт их использования для идентификации субъекта.

Система архивного видеонаблюдения в общем случае предназначена для наблюдения и документирования обстановки на объекте с целью последующего контроля и возможного расследования инцидентов безопасности. То есть сама по себе система видеонаблюдения не используется непосредственно для идентификации субъекта по его биометрическим данным. Если же происходит инцидент и начинается расследование, то идентификация правонарушителя по видеозаписи осуществляется уже в рамках уголовного или административного производства работниками компетентных государственных органов, а вовсе не как часть процесса видеонаблюдения.

Третья проблема при использовании системы видеонаблюдения — возможность использования архивных видеозаписей как доказательства чьей-либо противоправной деятельности. Имеется большое количество случаев, когда суды[3] признавали в качестве доказательства представленные стороной обвинения видеозаписи камер систем видеонаблюдения. Однако в большинстве случае для этого в рамках предварительного следствия назначается экспертиза видеозаписей на предмет отсутствия признаков монтажа. Производство такой экспертизы требует, как правило, много времени и средств.

К счастью, на эту проблему уже обратили внимание разработчики современных систем хранения видеоданных. Многие вендоры предлагают системы, где подлинность хранимых цифровых видеозаписей гарантируется с помощью специальных алгоритмов: при записи файла в систему происходит расчет его хэш-функции, запись ее в метаданные и при необходимости удостоверение электронной подписью. Каждый раз при обращении к видеозаписи происходит сверка хэш-функций, что подтверждает ее подлинность. Механизм расчета хэш-функций может быть сконфигурирован, исходя из корпоративных требований к стандартам шифрования. Очевидно, что использование видеозаписей, полученных из таких систем, не потребует долгой и дорогостоящей экспертизы.

По определению малополезны в качестве доказательства противоправных действий аналоговые видеозаписи, созданные с помощью дешевых камер систем оперативного видеонаблюдения. Если правонарушители не задержаны с поличным, то в дальнейшем у них есть прекрасная возможность отрицать свое участие в противоправных действиях.

[3] Автору известно, что в Российской Федерации нет прецедентного права. Тем не менее наши судьи активно используют передовой опыт своих коллег.