Предисловие ко 2-му изданию

Системы видеонаблюдения (СВН) занимают важное место в общей структуре интегрированных (комплексных) систем обеспечения безопасности объектов и физических лиц. Подобные системы в последнее время используются очень широко для охраны объектов и периметров, для контроля поведения посетителей, для наблюдения за производственными процессами и во многих других областях. Как правило, при охране реального объекта современные СВН интегрированы в комплексную охранную систему обеспечения безопасности вместе с системами контроля и управления доступом (СКУД) и охранно-пожарной сигнализации, хотя, конечно, они могут быть установлены и независимо.

Основные функции СВН — вести видеомониторинг определенных участков территории объекта и предоставлять визуальную информацию в виде, удобном для восприятия оператором службы безопасности, и для дальнейшей обработки и хранения. Поскольку задачей видеонаблюдения в структуре технических средств обеспечения безопасности является недопущение проникновения на охраняемый объект посторонних лиц, основными местами использования СВН являются двери, проходы, въездные ворота, периметр ограждения, а также подъездные пути и прилегающая территория. Внутри помещений объектами внимания традиционно являются внутренние двери, лестничные клетки, площадки около лифтов, входы в технические помещения и др. В случае необходимости решения специфических задач службы безопасности (например, в торговом предприятии или офисном помещении) видеокамеры СВН могут быть нацелены на определенные важные зоны, например, зону приема посетителей или зону совершения кассовых операций. Кроме того, материалы видеонаблюдения часто являются важнейшей фактической основой проведения служебного расследования, а в некоторых случаях единственным достоверным и независимым свидетельством как элемент судебных разбирательств.

Конструктивно современные СВН состоят из видеокамер различного уровня технологической сложности, средств обработки сигналов и их регистрации, комплекса устройств отображения изображения (видеомониторов) и устройств управления. Как правило, СВН имеют автономное электропитание и защищенные от посто-

роннего вторжения каналы связи. Благодаря современным компьютерным технологиям оператор службы безопасности имеет возможность воспринимать информацию со всех установленных видеокамер, управлять ими (поворачивать и увеличивать изображение) в масштабе реального времени, автоматически фиксировать поступающую визуальную информацию на жесткий диск компьютера и т. п.

Иногда видеокамеры дополняются устройствами обнаружения (детектирования) движения — в этом случае запись изображения может вестись не постоянно, а по моменту возникновения движения в подконтрольном пространстве (соответственно, автоматически прослеживая движение и обращая внимание оператора на возникшую ситуацию). К числу дополнительных возможностей СВН относится расширение спектра фиксируемой информации об окружающем пространстве за счет регистрации аудиоинформации, поступающей с внешних микрофонов.

Одним словом, СВН является одной из основ информационного обеспечения оперативной работы службы безопасности.

Видеонаблюдение, так же как и промышленное, транспортное, подземное и подводное телевидение и другие системы, относится к телевизионным системам специального назначения. По-другому эти системы называют прикладными замкнутыми телевизионными системами CCTV (Closed Circuit Television), т. е. предназначенными для ограниченного числа зрителей, в противоположность системам вещательного телевидения.

Одно из назначений книги — дать читателю необходимые знания для осознанного проектирования СВН и для оптимального подбора оборудования таких систем, без чего их реальное проектирование невозможно.

Надо отметить, что бытующее рассмотрение технических характеристик СВН в отрыве от реальных условий их эксплуатации зачастую приводит к низкой эффективности использования подобных систем. Поэтому значительное место в книге уделено практической стороне вопроса, в частности, оптимальному размещению видеокамер и выбору зон их обзора.

Как правило, в книге сознательно не упоминаются технические характеристики и описания конкретных моделей компонентов видеооборудования (объем книги не позволяет вместить все представленное на российском рынке их многообразие). К тому же стремительное изменение парка оборудования СВН, непрерывное появление новых образцов приборов неизбежно привело бы к быстрой потере актуальности книги.

Следует обратить внимание читателя на то, что с целью сохранения цельности и последовательности изложения материала в книге приведено описание ряда основополагающих, но уже устаревших компонентов СВН, понимание принципов работы которых облегчает переход к освоению современных устройств.

Содержательная часть второго издания книги включает десять глав.

В главе 1 приводятся общие сведения о СВН: решаемые ими задачи, принципы и способы их построения, классификация и правовые аспекты их применения, основные нормативные документы в области видеонаблюдения. Рассказывается также об основных сигналах, используемых в СВН.

В главе 2 рассматриваются основные технические характеристики компонентов СВН и их взаимосвязь.

Глава 3 посвящена цифровым и сетевым СВН, в том числе использованию в них компьютерных и сетевых технологий.

В главе 4 рассматриваются методы тестирования оборудования СВН и приводятся простейшие способы оценки работоспособности и качества используемых приборов.

Глава 5 посвящена вопросам проектирования СВН, в том числе особенностям выбора и расположения их компонентов и составлению технического задания.

В главе 6 приводятся практические сведения о применении СВН в различных сферах: в жилых зонах, на объектах торговли, на транспорте и др.

В главе 7 рассматривается ряд важных вопросов управления видеонаблюдением и применения в СВН облачных технологий.

Глава 8 посвящена рассмотрению актуальных на сегодняшний день вопросов применения в СВН интеллектуальной видеоаналитики.

В главе 9 идет речь о видеопереговорных устройствах (видеодомофонах).

Наконец, в главе 10 даются рекомендации по монтажу и техническому обслуживанию СВН и видеодомофонов.

Книга рекомендована специалистам, занимающимся проектированием и эксплуатацией СВН, сотрудникам фирм-поставщиков и фирм-заказчиков оборудования, слушателям курсов повышения квалификации и переподготовки специалистов, а также может быть полезна студентам технических университетов и других учебных заведений соответствующих специальностей и направлений.

Материал книги рассчитан на интересующегося читателя, знакомого с основами электроники, цифровой и телевизионной техники

и желающего самостоятельно приобщиться к такой увлекательной сфере техники как видеонаблюдение.

При написании второго издания книги автором частично были использованы материалы выпущенного в 2013 г. первого издания, в котором был отражен опыт преподавания им в свое время на курсах повышения квалификации МИПК МГТУ им. Н.Э. Баумана по программе «Устройство и техническое обслуживание систем видеонаблюдения». Для второго издания книга была существенно переработана и дополнена, но ее структура и характер изложения материала остались прежними. Переработка коснулась всех глав.

Автор выражает признательность рецензентам доктору технических наук, профессору В.А. Вороне и техническому директору ООО Axis Communications по Восточной Европе, России и СНГ П.А. Рожкову за полезные замечания, устранение которых во многом способствовало улучшению книги. Особую благодарность автор и издательство выражают ведущему российскому специалисту в области систем видеонаблюдения, генеральному директору фирмы «Мост безопасности» (г. Санкт-Петербург) Ю.М. Гедзбергу за ценные рекомендации и любезно предоставленную возможность использования принадлежащих ему материалов.

1 Общие сведения о системах видеонаблюдения

1.1. Построение систем видеонаблюдения и решаемые ими задачи

Системы видеонаблюдения предназначены для повышения уровня безопасности объекта и для минимизации возможных последствий нежелательных воздействий на людей, на материальные ценности и на информационные ресурсы. Нежелательные воздействия из внешней (по отношению к охраняемой зоне) среды могут быть как осознанными (со стороны криминальных элементов), так и результатом техногенных катастроф или стихийных бедствий. В общем виде СВН условно можно рассматривать как замкнутую систему управления (рис. 1.1), состоящую из ряда устройств.

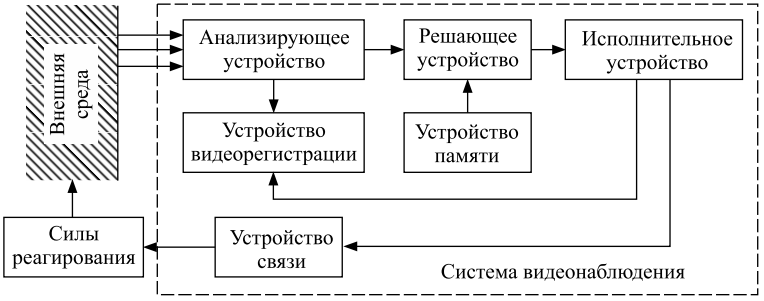

Рис. 1.1. Построение системы видеонаблюдения

Анализирующее устройство воспринимает воздействие из внешней среды (оптическое изображение объекта на матрице видеокамеры) и преобразует его в вид, приемлемый для принятия решения, т. е. по сути является системой получения сигналов телевизионных изображений (видеосигналов).

Устройство памяти хранит априорную информацию о возможной опасности. Например, оно «помнит» изображения «своих», учитывает характерные признаки опасных субъектов, «знает», в какое время в контролируемой зоне могут находиться люди, а когда не должны, и т. п. В устройстве памяти электронного прибора или компьютера могут храниться пороговые значения напряжения или кода,

соответствующие тревожной ситуации, информация о разрешенных временных «окнах» и пр.

Решающее устройство, на входы которого приходят сигналы с двух предыдущих устройств, формирует сигнал тревоги при выполнении установленных условий — в этом случае реализуется функция видеоконтроля. Если ранее эту функцию выполнял оператор, то в последнее время ему на помощь все больше приходят такие технические средства, как детекторы движения, детекторы оставленных или унесенных предметов, системы автоматического распознавания лиц людей или государственных регистрационных знаков (ГРЗ) автомобилей. Если на выходе анализирующего устройства (на экране видеомонитора) присутствует изображение контролируемой зоны, то в этом случае реализуется функция видеонаблюдения. Если решающим устройством является электронное устройство, в частности, компьютер, то на выходе анализирующего устройства должен быть соответствующий видеосигнал. Таким образом, решающее устройство вырабатывает сигнал для исполнительного устройства.

Исполнительное устройство может автоматически воздействовать на внешнюю среду — по тревоге включать сирену, строб-вспышку, исполнительные механизмы и т. п., а кроме того, оно может включать устройство видеорегистрации, а также управлять работой устройства связи.

Устройство видеорегистрации служит для организации протокола событий, т. е. записи видеосигналов, поступающих с анализирующего и исполнительного устройств, что в дальнейшем позволяет проводить расследование произошедших событий. Кроме того, видеозапись позволяет уменьшить влияние «человеческого фактора» охраны на обеспечение безопасности.

Устройство связи служит для передачи тревожной информации силам реагирования. Передача информации может осуществляться с помощью локальных компьютерных сетей, Интернета, электронной почты, телефонных сетей, SMS-сообщений и пр.

Функционирование сил реагирования (охрана, МЧС и т. п.), непосредственно воздействующих на негативные явления внешней среды с целью минимизации потерь в охраняемой зоне, непременно должно учитываться в работе СВН. Как показывает опыт, без учета их работы (так называемого «человеческого фактора») СВН может превратиться в бесполезный комплект дорогостоящего оборудования.

Эффективность системы обеспечения безопасности определяется скоростью ее отработки на внешние воздействия: для исключения развития событий по неблагоприятному сценарию скорость ответ-

ных действий сил реагирования должна быть выше, чем скорость нежелательных воздействий из внешней среды. С этой целью для торможения действий криминальных элементов используются средства механической укрепленности объекта и вандалозащищенности оборудования СВН (специальные крепления, скрытая прокладка кабелей, антитамперные датчики и др.), поскольку для их нейтрализации злоумышленникам требуется время. С этой же целью применяется резервное электропитание.

Кроме того, следует иметь в виду, что такие параметры эффективности СВН, как необходимая разрешающая способность и скорость обновления визуальной информации, определяются конкретной задачей, вытекающей из особенностей установки видеокамер.

Преимущество СВН по сравнению с другими системами обеспечения безопасности заключается в их высокой информативности (90 % всей информации об окружающем мире человек получает благодаря органам зрения). Проверить правильность функционирования систем обеспечения безопасности, убедиться в реальности тревоги, выработанной сигнализацией (охранной, пожарной, периметровой, антикражевой, автомобильной), можно не только посещением человеком места происшествия, но и дистанционно — с помощью видеонаблюдения. Еще важнее предотвратить происшествие, обнаружив опасное движение на подступах к охраняемой зоне, расшифровав возможную угрозу по экрану видеомонитора, что особенно актуально для удаленных необслуживаемых объектов. И с этим видеонаблюдение также успешно справляется.

Несовершенство любой из систем обеспечения безопасности в отдельности приводит к стремлению взаимного дополнения, некоего симбиоза систем, к попыткам проектировщиков интегрировать различные системы в единую систему обеспечения безопасности, чтобы существенно уменьшить влияние слабых сторон каждой из них, повысить достоверность получаемой оператором информации. Интеграция СВН (на аппаратном и/или программном уровне) с другими системами — это путь повышения уровня безопасности. При этом, однако, нельзя не учитывать вопросы живучести подобной централизированной системы, а также возможности работы оператора в условиях избытка информации, его физиологические ограничения обрабатывать потоки информации.

Важно также отметить, что главной задачей видеонаблюдения является не столько получение качественного изображения на экране видеомонитора, сколько возможность выработки достоверного суждения о наличии тревожной ситуации. В этом плане искажения изображения, недопустимые в вещательном телевидении, зачастую

оказываются вполне приемлемыми в СВН, а именно:

- частота смены кадров может быть и ниже 25 Гц;
- вместо обработки двух полей может обрабатываться только одно поле;
- цветопередача и передача градаций серого могут несколько отличаться от естественной;
- нелинейные или геометрические искажения не играют существенной роли.

С другой стороны, приобретают значимость некоторые характеристики, не столь важные в вещательном телевидении, например возможность оператору контролировать изображение на экране видеомонитора под острым углом обзора к его экрану или возможность круглосуточной эксплуатации оборудования в реальных обстоятельствах жизни и деятельности человека с учетом влияния окружающей среды.

Без преувеличения можно назвать революционным направлением в развитии СВН широкое практическое применение цифровых и сетевых систем. Это позволило вывести решение некоторых задач на качественно новый уровень, ранее не доступный при использовании аналогового оборудования. Благодаря возможностям цифровой обработки изображений и поиску оптимальных по соотношению цена/качество каналов передачи информации, появились новые направления применения СВН — использование их в расчетных кассовых узлах торговых предприятий, банкоматах, для распознавания ГРЗ автомобилей, идентификации людей и др.

Вследствие прикладного характера СВН их технические решения диктуются возможностью и экономической эффективностью практической реализации. В частности, одним из важнейших параметров СВН является удобство их монтажа и ввода в эксплуатацию, благодаря чему может использоваться максимум стандартных решений, облегчающих и ускоряющих инсталляцию.

Технические решения, заложенные в современных СВН, минимизируют трудоемкость работы монтажника, а, значит, и возможные его ошибки.

1.2. Правовые аспекты применения систем видеонаблюдения

В области использования СВН, наряду с техническими, функциональными и организационными, существуют и правовые аспекты.

Действующее российское законодательство не запрещает физическим и юридическим лицам использовать видеонаблюдение с целью обеспечения личной безопасности, сохранности имущества, а

также соблюдения трудовой дисциплины. Однако, поскольку вопросы его использования являются сравнительно новыми для российского правосудия, споры о допустимости видеозаписей в каждом конкретном случае все еще носят несистемный характер. В то же время видеозапись, произведенная на законных основаниях, может использоваться в качестве доказательств и системами видеонаблюдения, где могут быть задокументированы обстоятельства целого ряда преступлений — умышленной порчи имущества, хищений, телесных повреждений, убийств и др.

В ряде случаев использование СВН может быть ограничено или вообще запрещено законодательством. Поэтому их установщику имеет смысл ознакомиться с рекомендациями, которые затрагивают следующие аспекты:

- цель установки СВН, т. е. отсутствие ее противоречия местному законодательству. Таким образом, без должного обоснования цели видеонаблюдения оно может оказаться вне закона. Кроме того, следует помнить, что законность цели не существует в изоляции от конституционных прав граждан, в первую очередь от права на защиту частной жизни. Необходимо, кстати, помнить, что она подразумевает не только семейную, личную и интимную сферу жизни человека, поэтому требование о неприкосновенности должно быть соблюдено и во время нахождения гражданина и на рабочем месте;
- место размещения оборудования, т. е. обеспечивает ли оно видеонаблюдение только за разрешенными участками и объектами и не установлено ли оно в запрещенных местах. А поскольку сбор сведений о частной жизни граждан без их разрешения запрещен, в местах, где устанавливаются видеокамеры, должны быть размещены предупреждающие знаки (пример такого знака приведен на рис. 1.2), которые информируют о том, что на данной территории проводится видеонаблюдение;
- качество изображения, т. е. могут существовать ограничения применимости видеозаписей как доказательства в суде;
- хранение и доступ к видеозаписям, т. е. могут существовать ограничения на то, сколько времени разрешено их хранить, кому и где можно их просматривать;
- лицензирование, т. е. необходимость приобретения лицензии, разрешающей видеонаблюдение;
- регулярные проверки СВН, т. е. могут существовать рекомендации по их регулярной проверке для гарантии корректной работы входящего в их состав оборудования и др.

Рис. 1.2. Пример предупреждающего знака об установке системы видеонаблюдения

Таким образом, несмотря на очевидные выгоды от видеонаблюдения, каждый, кто осуществляет его организацию, должен отдавать себе отчет в том, что оно должно производиться на законных основаниях.

Рассмотрим наиболее важные юридические документы, регламентирующие использование видеонаблюдения.

Это прежде всего Конституция РФ, в ч. 1 статьи 23 которой сказано в том числе, что каждый гражданин имеет право на неприкосновенность частной жизни. При размещении видеокамер необходимо обязательно соблюдать требования, гарантирующие гражданам право на личную тайну, защиту доброго имени и чести. Поэтому установка видеокамер в таких местах, как, например, раздевалки, медпункты, туалеты и т. п. является незаконной.

Статья 24 Конституции гласит в том числе: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются», а в комментариях к ней сказано: «Конституция, устанавливая право искать, получать, передавать, производить и распространять информацию в соответствии с международными нормами, предусмотрела ограничения этого права, направленные на защиту личной жизни, уважение прав и репутации других лиц». Конституция устанавливает в качестве обязательного условия сбора, хранения, использования и распространения информации о частной жизни лица согласие этого лица. Однако некоторые руководители считают, что ничего личного на работе быть не может, и, устанавливая видеокамеры в офисах, не спрашивают согласия сотрудников и зачастую вообще не ставят их в известность о ведущемся видеонаблюдении.

Конституция устанавливает только общее правило, из которого, однако, существуют исключения, закрепленные в соответствующих законодательных актах. Так, не требуется согласия лица на сбор, хранение, использование и распространение сведений о нем при проведении следствия, дознания, оперативно-розыскных мероприятий. Порядок работы правоохранительных органов с информацией персонального характера регулируется прежде всего уголовно-процессуальным законодательством.

Перейдем теперь к Федеральным законам (ФЗ) и кодексам Российской Федерации, которые затрагивают вопросы видеонаблюдения.

В соответствии с п. 1 статьи 22 Федерального закона от 27.07. 2006 г. № 152-ФЗ «О персональных данных», все сведения, на основании которых может быть выполнена идентификация личности, приравниваются к персональным. Вместе с тем, использование СВН на объекте с целью контроля обстановки не подпадает под действие данной правовой нормы, так как следует разделять два процесса: мониторинг ситуации с помощью видеокамер и идентификацию субъекта по видеозаписи на основании его биометрических данных. Кстати, необходимо знать, что право такой идентификации имеют лишь сотрудники государственных органов в рамках выполнения ими оперативно-розыскных мероприятий.

В статье 6 Федерального закона от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» содержится норма включения в перечень оперативно-розыскных мероприятий видеонаблюдения, предполагающего использование СВН, а также других технических средств. Право на осуществление данного вида деятельности согласно статье 13 этого же ФЗ предоставлено органам внутренних дел (МВД), Федеральной службе безопасности (ФСБ), органам исполнительной власти в области государственной охраны, таможенным органам, службе внешней разведки (СВР), Федеральной службе исполнения наказаний (ФСИН) и др. Кроме того, сотрудники данных органов могут на законных основаниях использовать аппаратуру, предназначенную для скрытой съемки.

На заре эпохи видеонаблюдения не имелось юридической основы для постоянного правового контроля над ним в общественных местах. Такая ситуация существовала до тех пор, пока не вступил в силу Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 08.06.2020 г.) «Об информации, информационных технологиях и о защите информации», после чего для видеонаблюдения стали использоваться те же правовые нормы, что и для обработки личной информации на компьютере. В настоящее время уже не имеется правовых препятствий для установки СВН при условии их соответствия требованиям указанного ФЗ.

Стандарты, отвечающие требованиям этого закона, должны исходить из ряда принципов защиты информации, согласно которым она должна:

- использоваться справедливо и в соответствии с законом;
- использоваться для ограниченных целей и в полном соответствии с этими целями;
- быть адекватной, обоснованной и не избыточной;
- удовлетворять международным стандартам;
- быть точной и достоверной;

- храниться не дольше необходимого времени;
- использоваться в соответствии с правами личности;
- быть максимально защищенной от несанкционированного доступа;
- не передаваться в другие страны без надлежащей защиты.

Правовые аспекты видеонаблюдения отражены в ряде кодексов Российской Федерации.

В случае совершения противоправных действий, зафиксированных видеокамерой, идентификация лица, совершившего правонарушение, проводится в рамках процедуры дознания, которая регламентируется Уголовно-процессуальным кодексом (УПК) РФ и Кодексом административного судопроизводства (КАС) РФ.

Так, статьи 81, 84 УПК РФ содержат положения, согласно которым видеозаписи являются документами, с помощью которых можно установить процесс совершения преступления, а также иные детали, относящиеся к уголовному делу. В настоящее время в российских следственных и судебных органах видеозаписи используются в качестве доказательств в рамках уголовного процесса.

Статья 55, ч. 2 Гражданского процессуального кодекса (ГПК) РФ также устанавливает, что видеозаписи могут использоваться в качестве доказательства в судебном разбирательстве. Например, известны случаи подачи гражданских исков к гостиницам, торговым центрам или офисным комплексам. В свою очередь, компания, которой принадлежат помещения с установленными в них видеокамерами, может стать инициатором судебного разбирательства в отношении физических лиц, например предъявление исков к клиентам или к своим работникам о возмещении ущерба.

Важно также помнить, что статья 138.1 Уголовного кодекса (УК) РФ запрещает незаконные производство, приобретение и/или сбыт специальных технических средств, предназначенных для негласного получения информации. Поэтому приобретение таких, казалось бы, невинных вещей, как например авторучка, наручные часы или зажим для галстука со встроенной скрытой видеокамерой, которые на первый взгляд кажутся безобидными, может грозить санкциями покупателю. Статья же 137 УК РФ предусматривает запрет на осуществление незаконного сбора либо распространения сведений, касающихся частной жизни лиц без получения их согласия.

Кодекс РФ об административных правонарушениях (КоАП) в статье 26.7, ч. 2 также предусматривает возможность использования видеозаписей в качестве доказательств. В административном производстве по делам о мелком хулиганстве, порче имущества на незначительную сумму и т. п. также допустимо использовать такие

материалы. В качестве допустимых процессуальных доказательств называет видеозаписи и статья 64, ч. 2 Арбитражного процессуального кодекса (АПК) РФ.

Согласно статье 21 Трудового кодекса (ТК) РФ в его ред. от 09.11.2020 г., введенной Федеральным законом от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации», работник имеет право на полную и достоверную информацию об условиях и охране труда на рабочем месте. А вот в соответствии со статьями 192, 193 ТК РФ негласно полученная работодателем видеозапись не может являться основанием для наложения дисциплинарной ответственности на работника в виде увольнения. В случае его добровольного согласия, что должно быть зафиксировано в письменном виде, руководство имеет право на ведение видеонаблюдения на рабочем месте. При этом не должно быть противоречий с уже упомянутым законом № 152-ФЗ, законодательством о государственной тайне и другими нормативными актами.

На промышленных предприятиях СВН могут устанавливаться с целью обеспечения безопасности и контроля за качеством выпускаемой продукции и соблюдением трудовой дисциплины. Тем не менее, как уже было сказано выше, вне зависимости от цели видеонаблюдения установка записывающей техники и там должна быть осуществлена с учетом законодательных норм о неприкосновенности частной жизни граждан. Чтобы избежать судебных разбирательств и обеспечить соблюдение норм закона, руководство предприятия обязано ознакомить всех сотрудников с приказом о запуске СВН, а также получить их письменную отметку о согласии. Кроме этого, во всех помещениях, где осуществляется видеонаблюдение, требуется разместить предупреждающий знак (см. выше) с уведомлением о том, что оно ведется.

Правила организации видеонаблюдения на предприятиях распространяются и на офисные помещения. В этой связи в договоре о найме специалистов должно быть указано то, что они согласны с ведением видеонаблюдения на рабочем месте. При несоблюдении же работодателем правил организации видеонаблюдения он может оказаться в неприятных ситуациях — от потери лояльности сотрудников, узнавших об этом, до проигрыша дела в суде. Но если видеонаблюдение ведется с соблюдением всех правовых норм, видеозапись помогает не только обеспечить безопасность, но дает возможность контролировать и оптимизировать бизнес-процессы.

Важно отметить, что на сегодняшний день законодательство не включает работы по установке СВН в перечень видов деятельности, подлежащих обязательному лицензированию. Однако в ряде случа-