



Утверждено
Генеральный директор
ООО «Инкерман»
Даль К.Ю.
«09» января 2024 г.

ПОЛОЖЕНИЕ
о системе видеонаблюдения
в Обществе с ограниченной ответственностью «Инкерман»
(ООО «Инкерман»)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано в соответствии со ст.ст. 23, 24 Конституции Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 06.03.2006 г. № 35-ФЗ «О противодействии терроризму», Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах здоровья граждан РФ».

1.2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеoinформации об объектах и помещениях, а также запись полученного изображения со звуком и его хранение для последующего использования.

1.3. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности работников и посетителей организации и не может быть направлена на сбор информации о конкретном человеке.

1.4. Система открытого видеонаблюдения в ООО «Инкерман» (далее по тексту - Организация) является элементом общей системы безопасности Организации, направленной на обеспечение безопасной организации оказания медицинских услуг, поддержание дисциплины и порядка в Организации, предупреждение возникновения чрезвычайных ситуаций и обеспечение сохранности имущества.

1.5. Настоящее Положение обязательно для работников, пациентов и (или) посетителей ООО «Инкерман». Настоящее Положение подлежит размещению на официальном сайте Организации и находится в свободном доступе для работников и посетителей ООО «Инкерман».

1.6. С целью противодействия терроризму и совершению противоправных действий, ООО «Инкерман» обязано вести наблюдение за состоянием обстановки на всей территории, архивировать и хранить данные в течение 30 дней (постановление Правительства от 13.01.2019 г. № 8). Система видеонаблюдения в медицинской организации необходима для защиты посетителей и персонала от угроз терроризма и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009г. № 384 «Технический регламент о безопасности зданий и сооружений»), контроля за соблюдением трудовой дисциплины и связанных с исполнением работниками должностных обязанностей, контроля и учета рабочего времени, требований охраны труда и мер безопасности, обеспечения сохранности имущества организации и работников, а также контроля качества и повышения сервиса оказываемых в организации медицинских услуг.

2. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

2.1. Решение об установке системы видеонаблюдения принимается генеральным

директором Организации, видеоконтроль вводится соответствующим приказом.

2.2. Лица, являющиеся сотрудниками организации на момент введения системы видеоконтроля, должны в письменной форме выразить свое согласие или несогласие на введение данной системы.

2.3. Сотрудники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на обработку персональных данных.

2.4. Посетители организации информируются о системе видеоконтроля путем размещения специальных информационных табличек на входах в зону видимости камер.

2.5. Система видеонаблюдения Организации включает в себя ряд устройств: камеры, микрофоны, записывающие устройства.

2.6. Места установки видеокамер в Организации определяются по мере необходимости в соответствии с конкретными задачами.

2.7. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры), а также в помещениях, где оказываются медицинские услуги (процедурный кабинет, кабинеты врачей и т.п), кабинетах сотрудников.

2.8. Установка видеокамер не допускается в туалетных комнатах, комнатах для переодевания работников и в иных местах, связанных с осуществлением личных нужд работников, посетителей.

2.9. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

3.1. Целью системы видеонаблюдения является создание условий для антитеррористической защищенности в Организации, безопасности персонала и пациентов, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, осуществление внутреннего контроля качества и безопасности медицинской деятельности, контроля за соблюдением трудовой дисциплины и связанных с исполнением работниками должностных обязанностей, контроля и учета рабочего времени, требований охраны труда.

3.2. Задачами организации видеонаблюдения являются:

- контроль за обстановкой в помещениях и на территории Организации, обеспечение защиты от несанкционированного проникновения на территорию и в здание посторонних лиц и транспортных средств;
- своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории Организации;
- охрана жизни, предупреждение и минимизация рисков травматизма работников Организации и посетителей;
- установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником);
- обеспечение противопожарной защиты зданий и сооружений;
- повышение ответственности всех сотрудников за качество своей профессиональной деятельности и выполнение должностных обязанностей;
- раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;
- пресечение противоправных действий со стороны работников Организации и посетителей;
- охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а также предупреждение случаев хищения

имущества организации и/или работников/посетителей;

- отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;

- информационное обеспечение принятия решений генеральным директором Организации.

- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3.3. Система видеонаблюдения должна обеспечивать:

- видео фиксацию текущего состояния объекта видеонаблюдения;

- сохранение архива видеозаписей для последующего анализа;

- воспроизведение ранее записанной информации;

- копирование сохраненных записей на внешние носители;

- оперативный доступ к архиву видеозаписей за конкретный период времени и с определённых видеокамер.

3.4. В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, будут использованы в качестве доказательства в уголовном или гражданском судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

4.2. Организация обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами.

4.3. Обработка персональных данных должна осуществляться на законной основе и ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

4.4. Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

5. ПРОСМОТР, ХРАНЕНИЕ ДАННЫХ ВИДЕОНАБЛЮДЕНИЯ И ПЕРЕДАЧА ДАННЫХ ТРЕТЬИМ ЛИЦАМ

5.1. Запись камер видеонаблюдения осуществляется постоянно (24 часа в сутки) и подлежит хранению в сроки от 30 до 90 дней, в зависимости от технических возможностей оборудования.

5.2. Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора, которая уничтожается автоматически по мере заполнения памяти жесткого диска через 30 - 90 дней. Запись видеонаблюдения является конфиденциальной. В случае необходимости возможно копирование видеозаписей, полученных камерами видеонаблюдения на внешние носители при письменном запросе следственных или судебных органов.

5.3. Доступ к просмотру записей видеонаблюдения, хранящимся установленный

период на жестком диске видеорегистратора, имеет генеральный директор Организации, главный врач и главный инженер.

5.4. По согласованию с генеральным директором другие работники Организации могут быть допущены к просмотру записей видеонаблюдения, пространственных зон, связанных с их должностными обязанностями, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц. Для получения доступа к системе видеонаблюдения сотрудник получает учетную запись. Каждая учетная запись включает логин и пароль.

5.5. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора, который известен лицам, имеющим право на просмотр.

5.6. Доступ к просмотру видео с камер наблюдения (а также скриншотов и любых других копий) осуществляется только тем сотрудником, который является владельцем учетной записи. Сотруднику запрещается предоставлять любым другим лицам возможность просмотра видео с камер под его учетной записью даже в его присутствии с его устройства. Не допускается просмотр видео с камер совместно с посторонними лицами или с сотрудниками Общества за исключением целей обучения подчиненных или анализа их работы, а также для разбора служебных действий своих подчиненных.

5.7. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному запросу следственных и судебных органов, а также по письменному запросу работников, изображенных на видеозаписи). Вопрос о передаче записей решает генеральный директор Организации.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных подлежат возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

6.3. Работникам Организации запрещается: препятствовать работе системы видеонаблюдения путем регулировки направления (обзора) камер видеонаблюдения, загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер системы видеонаблюдения. За причинение материального вреда и порчу камер системы видеонаблюдения работники Организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее положение является локальным нормативным актом, принимается, утверждаются приказом директора Организации.

7.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии с действующим законодательством Российской Федерации.

7.3. Ознакомление работников учреждения с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под подпись.