УТВЕРЖДАЮ

Генеральный директор

ООО «Инвестмедком»

_____О.С.Манюхина

«01» «октября» 2019г.

ПОЛОЖЕНИЕ О СИСТЕМЕ ВИДЕОНАБЛЮДЕНИЯ В ООО «ИНВЕСТМЕДКОМ»

1. Общие положения

1.1 Положение о системе видеонаблюдения (далее Положение) разработано в соответствии со статьями 23 и 24 Конституции Российской Федерации, со статьями 152.1 и 152.2 Гражданского кодекса Российской Федерации, со статьей 77 Гражданского процессуального кодекса Российской Федерации, от 06.03.2006 №35-ФЗ «О противодействии терроризму», от 25.07.2002 № 114- ФЗ «О противодействии экстремистской деятельности», с Трудовым кодексом Российской Федерации (в том числе статьями 16, 21, 22, 86, 91, 209), с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее 152-ФЗ), с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением правительства РФ от 25.03.2015г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии РФ, и форм паспортов безопасности таких мест и объектов (территорий)».

1.2 Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеоинформации об объекте, помещениях, территории.

1.3 Техническое оснащение системы видеонаблюдения включает в себя камеры, мониторы, записывающие устройства (видеорегистраторы).

1.4 Система видеонаблюдения является элементом общей системы безопасности предприятия и может использоваться лишь на законных основаниях (борьба с возможными правонарушениями).

1.5 Система видеонаблюдения в центре является открытой и не может быть направлена на сбор информации о конкретном человеке.

1.6 Допускается ведение видеонаблюдения только с использованием стационарных видеокамер.

1.7 В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность работников на рабочем месте или в иных помещениях (территории), закрытых для общего доступа, видеонаблюдение считается обработкой биометрических персональных данных, в связи с чем не допускается ведение видеонаблюдения в местах закрытого доступа.

2. Цели и задачи системы видеонаблюдения

2.1 Видеонаблюдение в центре осуществляется с целью антитеррористической защищенности, охраны порядка, противопожарной защиты, пресечения и фиксации противоправных действий, с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имущественным и (или) неимущественным правам организации в целом, работников, контрагентов или пациентов.

2.2 На систему видеонаблюдения возлагаются следующие задачи:

2.2.1 антитеррористическая защищенность работников, контрагентов, пациентов;

2.2.2 охрана порядка и безопасности в центре;

2.2.3 противопожарная защита помещений и территории центра;

2.2.4 пресечение противоправных действий;

2.2.5 фиксация противоправных действий;

2.2.6 повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения;

2.2.7 минимизация рисков материальных потерь, сохранность личного имущества работников, имущества организации, имущества контрагентов и пациентов;

2.2.8 обеспечение личной безопасности работников;

2.2.9 контроль трудовой дисциплины и обеспечение объективности при

вынесении дисциплинарных взысканий;

2.2.10 обеспечение соблюдения организацией обязанностей, возложенных на него действующим законодательством Российской Федерации, в том числе по противодействию коррупции.

2.3 В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, могут быть использованы в качестве доказательства:

2.3.1 в уголовном, гражданском или административном судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие;

2.3.2 для доказывания факта совершения дисциплинарного проступка работником организации, а также для установления личности работника организации в момент совершения им соответствующего дисциплинарного проступка.

2.4. Материалы видеозаписей для идентификации личности могут быть переданы уполномоченным органам без письменного согласия субъекта персональных данных с целью противодействия терроризму, противодействия коррупции, с целью защиты правопорядка и т.п., то есть в случаях, предусмотренных частью второй статьи одиннадцать 152-ФЗ. Передача материалов видеозаписи осуществляется в соответствии с порядком, установленным для передачи сведений, содержащих персональные данные.

3. Порядок организации системы видеонаблюдения

3.1 Система видеонаблюдения в центре может быть установлена в общедоступных помещениях здания, расположенного по адресу г.Москва ул.Лестева, д.20, которые закреплены за ООО «Инвестмедком» на праве хозяйственного ведения (далее помещения) и (или) на праве аренды.

3.2 Решение об установке (снятии) системы видеонаблюдения принимается приказом генерального директора. При принятии решения по установке системы видеонаблюдения приказом генерального директора назначается лицом, ответственное за соблюдение законодательства Российской Федерации при эксплуатации данной системы (далее ответственный за видеонаблюдение).

3.3 Установка системы видеонаблюдения осуществляется в соответствии с еѐ целями и задачами.

3.4 В центре запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

3.5 Запрещается эксплуатация системы видеонаблюдения в туалетных комнатах, бытовых помещениях.

3.6 Запрещается использование видеонаблюдения для сбора, хранения, использования, распространения информации о частной жизни лица без его письменного согласия.

3.7 При обнаружении нарушения правил эксплуатаций системы видеонаблюдения ответственный за видеонаблюдение обязан немедленно доложить об этом генеральному директору, приняв соответствующие меры по приостановке еѐ эксплуатации.

3.8 Работники центра, пациенты должны быть надлежащим образом уведомлены о ведении на территории центра видеонаблюдения.

3.9 Работники центра до начала эксплуатации системы видеонаблюдения (впоследствии все вновь принимаемые работники) должны быть письменно ознакомлены с настоящим Положением.

.

4. Порядок ведения видеонаблюдения

4.1 Видеонаблюдение должно проводиться без идентификации снятых на видеозапись изображений людей. До передачи материалов видеосъемки для установления личности снятого человека видеонаблюдение не считается обработкой биометрических персональных данных и на еѐ проведение письменного согласия не требуется.

4.2 При установке системы видеонаблюдения уведомление о еѐ ведении осуществляется посредством размещения соответствующей информации в местах, обеспечивающих гарантированную видимость в дневное и ночное время, до входа в помещения и (или) на территорию центра. Такая информация должна содержать сведения об условиях внутриобъектового режима.

4.3 К просмотру видеоинформации допускаются:

4.3.1 работники охраны с целью выполнения возложенных на них охранных услуг. Работники охраны имеют право просмотра видеоинформации только в

режиме онлайн при исполнении возложенных на них обязанностей по охране центра в период своего рабочего времени (дежурства);

4.3.2 генеральный директор, его заместители с целью выполнения возложенных на них должностных обязанностей;

4.3.3 представители уполномоченных органов с целью использования изображений для осуществления государственных, общественных или иных публичных интересов. Представители уполномоченных органов допускаются до просмотра видеозаписей на основании письменного запроса, оформленного в соответствии с требованиями законодательства в сфере защиты персональных данных, с разрешающей резолюцией генерального директора или его заместителя, а также в присутствии уполномоченного должностного лица организации;

4.3.4 уполномоченные должностные лица организации на основании соответствующего приказа генерального директора.

4.4 Установка видеокамер производится в разрешенных помещениях центра в необходимом для осуществления видеонаблюдения количестве.

4.5 Отображение процесса видеонаблюдения должно производиться на мониторе, расположение которого исключает его просмотр сторонними лицами. Для помещений, в которых располагаются мониторы, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Места нахождения мониторов определяются приказом генерального директора.

4.6 Хранение видеозаписей осуществляется на видеорегистраторах, входящих в состав установленной в центре системы видеонаблюдения. Места нахождения видеорегистраторов определяются генеральным директором. Для помещений либо мест нахождения видеорегистраторов организуется режим обеспечения безопасности. В этих целях должна исключаться возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц либо места нахождения регистраторов должны быть закрыты на ключ и опечатаны.

4.7 Программное обеспечение, позволяющее просматривать видеозаписи с видеорегистраторов, должно быть защищено паролем доступа.

4.8 Приказом генерального директора назначается ответственный за ограничение доступа к видеозаписям.

Ответственный за ограничение доступа к видеозаписям обеспечивает хранение и использование полученных ключа, опечатывающего устройства и пароля доступа, исключающих несанкционированный доступ к видеозаписям.
С целью решения вопросов технического обслуживания оборудования Уполномоченному лицу предоставляется право самостоятельного доступа к видеозаписям и к месту нахождения видеорегистраторов с предварительного уведомления ответственного за видеонаблюдение.

4.9 Просмотр видеозаписей с установленных видеорегистраторов осуществляется на компьютере, установленном на посту охраны.
Лица, имеющие право доступа к просмотру видеозаписей, осуществляют их просмотр только в присутствии генерального директора.

4.10 В случае обнаружения несанкционированного доступа к видеорегистратору и (или) видеозаписи (срыв пломбы, взлом пароля) ответственное лицо в кратчайшие сроки обязан в письменной форме доложить о случившемся генеральному директору.

4.11 Копирование и (или) распространение видеозаписей не допускается, за исключением случаев, предусмотренных частью второй статьи 6 одиннадцать 152-ФЗ, а также в случае необходимости фиксации нарушения трудовой дисциплины.

4.12 Уничтожение видеозаписей производится в автоматическом режиме по мере заполнения памяти жесткого диска по истечении не более 30 календарных дней с момента записи, специальным техническим устройством, являющимся составной частью используемой системы видеонаблюдения.

5. Использование записей видеонаблюдения для контроля трудовой дисциплины

5.1 При возникновении необходимости просмотра видеозаписи для контроля трудовой дисциплины материалы видеозаписей для фиксации нарушения трудовой дисциплины и идентификации личности, допустившей нарушение, могут быть просмотрены уполномоченными должностными лицами организации.
Перечень уполномоченных должностных лиц определяется на основании соответствующего приказа генерального директора, в котором также должны быть обоснованы цели просмотра и полномочия должностных лиц, допущенных к просмотру видеозаписи.
Должностные лица, допущенные к просмотру, обязаны до начала просмотра дать письменное обязательство о неразглашении персональных данных, а после просмотра составить соответствующий акт.

Идентификация личности работника предприятия по видеозаписи уполномоченными должностными лицами может производиться только с письменного согласия субъекта персональных данных, взятом в порядке, определенном п.п. 5.7 настоящего Положения.

5.2 Копирование видеозаписи, содержащей фиксацию нарушения работником трудовой дисциплины (далее копия видеозаписи), допускается уполномоченным должностным лицом на учтенный съемный носитель с целью использования копии видеозаписи при проведении процедуры применения к работнику дисциплинарного взыскания.

5.3 Хранение копии видеозаписи осуществляется уполномоченным работником с соблюдением требований, установленных к хранению электронных документов, содержащих персональные данные.

5.4 Передача копии видеозаписи может осуществляться только уполномоченным органам (контрольно-надзорные органы, судебные органы) в порядке, установленном к передаче сведений, содержащих персональные данные.

5.5 Просмотр копии видеозаписи субъектом персональных данных возможен в случае отсутствия на данной копии видеозаписи изображения иных субъектов персональных данных.

5.6 Уничтожение копии видеозаписи производится в порядке, установленном к уничтожению документов по личному составу.

5.7 До начала ведения видеонаблюдения с целью фиксации возможных действий противоправного характера с работниками организации должны быть оформлены дополнительные соглашения об изменении условий заключенных трудовых договоров (введение видеонаблюдения) с соблюдением требований, предусмотренных статьей 74 Трудового кодекса Российской Федерации.
Во всех вновь заключаемых трудовых договорах необходимо включать условие о ведении на предприятии видеонаблюдения.

6. Техническое сопровождение ведения видеонаблюдения

6.1 Лицо, ответственное за ведение видеонаблюдения в центре, обязано своевременно принимать меры по устранению технических неполадок в работе соответствующего оборудования.

6.2 С целью минимизации технических сбоев в работе оборудования системы видеонаблюдения генеральный директор соответствующим приказом определят должностное лицо, ответственное за его техническое

обслуживание (ремонт). До начала проведения соответствующих работ данное должностное лицо должно дать письменное обязательство о неразглашении конфиденциальной информации, в том числе сведений, содержащих персональные данные.

6.3 Генеральный директор с целью технического обслуживания и ремонта оборудования системы видеонаблюдения имеет право заключить договорные отношения со специализированной организацией.

6.4 При заключении договорных отношений со сторонней организацией в проект договора необходимо вносить условие о неразглашении потенциальным контрагентом (его работниками) конфиденциальной информации (в том числе сведений, содержащих персональные данные), полученной при исполнении договорных обязательств.

7. Ответственность

7.1. Ответственность за соответствие технических характеристик устанавливаемого оборудования для ведения видеонаблюдения требованиям действующего законодательства Российской Федерации и настоящего Положения несет генеральный директор.

7.2 Ответственность за соблюдение требований законодательства Российской Федерации при определении помещений и (или) территории центра, в которых будет осуществляться ведение видеонаблюдения несет генеральный директор.

7.3 Ответственность за надлежащее уведомление о ведении на предприятии видеонаблюдения несет лицо, ответственное за ведение видеонаблюдения.

7.4 Ответственность за соблюдение действующего законодательства Российской Федерации и настоящего Положения при ведении видеонаблюдения несет ответственный за видеонаблюдение.

7.5 Ответственность за соблюдение законодательства в сфере защиты персональных данных при ведении видеонаблюдения несет лицо, назначенное соответствующим приказом ответственным за организацию обработки персональных данных.

7.6 Уполномоченные должностные лица несут персональную ответственность за разглашение сведений, содержащих персональные данные, полученных при просмотре видеозаписей.

7.7 Ответственность за соблюдение конфиденциальности информации,

полученной с видеокамер при предоставлении охранных услуг, несут сотрудники охраны, непосредственно осуществляющие охранные функции.