Приложение
к приказу №80д от 28.02.2024 г.

ПОЛОЖЕНИЕ
о системе видеонаблюдения в ГАУ РХ «Абаканский пансионат ветеранов»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В соответствии с требованиями Федерального закона от 06.03.2006 г. №35 «О противодействии терроризму», Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», Федерального закона от 02.07.2021 г. №311-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации», Постановления Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановления Правительства РФ от 13 мая 2016 г. N 410 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства труда и социальной защиты Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, и формы паспорта безопасности этих объектов (территорий)".

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

1.3. С целью противодействия терроризму и совершению противоправных действий, учреждение обязана вести видеонаблюдение за состоянием обстановки в режиме реального времени на всех территориях, помещениях, архивировать и хранить данные в течение 30 суток.

Система видеонаблюдения (далее – СВН) необходима для защиты (безопасности) персонала, проживающих и посетителей от угроз терроризма и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009 г. №384 «Технический регламент о безопасности зданий и сооружений»), а также внутреннего контроля качества и безопасности оказания социальных услуг.

1.4. СВН является открытой и не может быть направлена на сбор информации о конкретном человеке, направлена на контроль дисциплины сотрудников и порядка в учреждении, предупреждения возникновения чрезвычайных ситуаций и обеспечения сохранности имущества.

1.5. Настоящее Положение обязательно для работников, проживающих и (или) посетителей учреждения. Настоящее Положение подлежит размещению на официальном сайте и находится в свободном доступе для работников, проживающих и посетителей учреждения.

2. ПОРЯДОК ОРГАНИЗАЦИИ СВН

2.1. Решение об установке СВН принимается директором учреждения, видеоконтроль вводится соответствующим приказом.

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

2.3. Посетители учреждения информируются о СВН путем размещения специальных информационных табличек в зонах видимости видеокамер.

2.4. СВН учреждения входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства (видеорегистраторы).

2.5. Места установки видеокамер в учреждение определяются по мере необходимости в соответствии с конкретными задачами решением директора.

2.6. Видеокамеры устанавливаются в местах открытых для общего доступа (территория, входы в здание, коридоры).

2.7. Установка видеокамер не допускается в туалетных, душевых комнатах для проживающих и работников учреждения и в комнатах для переодевания работников.

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

2.9 Лица, ответственные за эксплуатацию, работоспособность и защиту информации в СВН назначаются приказом директора.

3. ЦЕЛИ И ЗАДАЧИ СВН

3.1. Целью СВН является создание условий для антитеррористической защищенности в учреждение, безопасности персонала и проживающих, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, осуществление внутреннего контроля качества и безопасности социальных услуг.

3.2. Задачами организации видеонаблюдения являются:

– контроль за обстановкой на территории и объектах учреждения, обеспечение защиты от несанкционированного проникновения на территории, в здания и в помещения посторонних лиц и транспортных средств;

– своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории учреждения;

– охрана жизни, предупреждение и минимизация рисков травматизма работников и проживающих;

– установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником, проживающим, посетителем);

– 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, проживающих и посетителей учреждения;

– охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а так же предупреждение случаев хищения имущества учреждения и/или работников/ посетителей/ проживающих;

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

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

3.3. СВН должна обеспечивать:

– видео фиксацию текущего состояния объекта видеонаблюдения;

– сохранение архива видеозаписей для последующего анализа;

– воспроизведение ранее записанной информации;

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

3.4. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, могут быть использованы в качестве доказательства в уголовном, гражданском или административном судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПОСТРАНЕНИЯ (СЛУЖЕБНОЙ ИНФОРМАЦИИ)

4.1. СВН позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой служебной информации.

4.2. Учреждение обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, в части касающейся предусмотренных Федеральным законом №152-ФЗ от 27.07.2007 года «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами.

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

5.1. СВН предполагает запись информации в режиме реального времени на жесткий диск видеорегистратора и резервного автоматизированного рабочего места (далее – АРМ), которая не подлежит

перезаписи и длительному хранению:

– для видеокамер, установленных для обеспечения антитеррористической защищенности учреждения, уничтожается автоматически по мере заполнения памяти жесткого диска не менее, чем через 30 суток;

– для видеокамер, установленных для осуществления внутреннего, контроля качества и безопасности оказания социальных услуг, уничтожается автоматически по мере заполнения памяти жесткого диска до 14 суток.

5.2. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жестких дисков видеорегистраторов и резервного АРМ, редактированию.

Исключение составляют случаи официального письменного обращения с разрешения директора учреждения.

5.3. Отображение процесса видеозаписи в режиме реального времени производится на экраны, установленные:

– в помещениях контрольно-пропускных пунктов, в которых оборудованы посты охраны на территориях учреждения, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;

– на посту охраны, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;

5.4. Разрешение доступа к просмотру записей видеонаблюдения, хранящихся установленный период на жестком диске видеорегистратора и резервного АРМ, осуществляется:

– для просмотров записей с разрешения заместителя директора по административно – хозяйственной работе, инженера инженерно – хозяйственного отдела, старшего сторожа (вахтера, начальника охраны);

На основании письменного разрешения директора учреждения другие работники учреждения могут быть допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц только в присутствии ответственного за организацию работы СВН или лица, его замещающего.

5.5. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора, который известен лицам, имеющим право на просмотр согласно пункту 5.4.

5.6.Просмотр записанных изображений может осуществляться исключительно при личном участии должностных лиц имеющих право на просмотр указанных в пункте 5.4. (при отсутствии посторонних лиц).

5.7. Для защиты публичных интересов (т.е. выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи и сотрудники полиции (других правоохранительные органы РФ).

5.8. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному мотивированному запросу следственных и судебных органов, а также по письменному мотивированному запросу работников, изображенных на видеозаписи).

5.9. Решение о передаче записей принимает директор учреждения.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона №152-ФЗ от 27.07.2007 года «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный и материальный 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 учреждения (кроме уполномоченных на то лиц) и охранной организации **ЗАПРЕЩАЕТСЯ:**

препятствовать работе СВН путем регулировки направления (обзора) камер видеонаблюдения, загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер СВН.

За причинение материального вреда и порчу камер СВН работники учреждения и охранной организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ОРГАНИЗАЦИЯ ВСЕСТОРОННЕГО ОБЕСПЕЧЕНИЯ РАБОТЫ СВН

7.1. Ответственность за проведение технического обслуживания, в том числе проведения ремонтных работ для поддержания работоспособности СВН возлагается на инженера инженерно – хозяйственного отдела.

7.2. Ответственность за работоспособность программно-аппаратного комплекса СВН, в том числе его модернизацию (обновление операционных систем, САВЗ, системы разграничения доступа и т.д.) возлагается на инженера инженерно – хозяйственного отдела.

7.3. Выполнение работ, указанных в п.п. 7.1. и 7.2., в том числе в нерабочее время (выходные, нерабочие и праздничные дни) проводить только по согласованию с ответственным за организацию работы СВН.

7.4. Ответственность за предотвращение неправомерного доступа к защищаемой информации, хранящейся на магнитных накопителях, контроль за ее использованием, возлагается на инженера инженерно – хозяйственного отдела.

7.5. Организация информационной безопасности при эксплуатации СВН должна обеспечивать установленные сроки хранения, конфиденциальность и целостность информации и обеспечивается проведением следующих мероприятий:

– ограничением круга лиц, допущенных к информации с СВН, в соответствии с приказом директора;

– ограничением физического доступа к магнитным накопителям СВН путем опечатывания устройств, исключающих их вскрытие без нарушения оттиска печати ответственного за организацию работы СВН по ЗИ;

– обеспечением учета доступа в помещения, где используются магнитные накопители СВН;

– обеспечением хранения и выдачи ключей от помещений, где используются магнитные накопители СВН с записью в журнале учета и выдачи ключей.

7.6. Руководители структурных подразделений в случае нарушения работоспособности СВН представляют заявки на их ремонт в установленном порядке.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение, изменения и дополнения к нему, утверждаются приказом директора учреждения.

Заместитель директора
по административно – хозяйственной работе С.В. Кузьмин