УТВЕРЖДЕНО
приказом Муниципального
бюджетного дошкольного
образовательного учреждения
детский сад «Солнышко» с.
Криничное Белогорского района
Республики Крым
от 23.11.2026 г № 234

# ПОЛОЖЕНИЕ

о системе видеонаблюдения Муниципального бюджетного дошкольного образовательного учреждения детский сад «Солнышко» с. Криничное Белогорского района Республики Крым

## 1. Общие положения

1.1. Настоящее Положение определяет цели, правовые основания, порядок организации и функционирования системы видеонаблюдения Муниципального бюджетного дошкольного образовательного учреждения детский сад «Солнышко» с. Криничное Белогорского района Республики Крым (далее соответственно – Положение, система видеонаблюдения, учреждение), порядок обработки и защиты персональных данных, получаемых с использованием системы видеонаблюдения, а также права субъектов персональных данных.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», постановлением Правительства Российской Федерации от 2 августа 2019 г. № 1006 «Об утверждении требований к антитеррористической защищённости объектов (территорий) Министерства просвещения Российской Федерации…», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, приказом ФСТЭК России от 18 февраля 2013 г. № 21, Трудовым кодексом Российской Федерации и уставом учреждения.

1.3. Система видеонаблюдения представляет собой совокупность видеокамер, устройств обработки, передачи и хранения видеоинформации, программного обеспечения и каналов связи, обеспечивающих формирование, передачу и хранение видеоизображений контролируемых зон.

1.4. Персональные данные, получаемые с использованием системы видеонаблюдения (видеоизображение физического лица, дата, время и место видеофиксации), обрабатываются в информационной системе персональных данных «Видеонаблюдение» и относятся к иным категориям персональных данных.

1.5. Видеонаблюдение является открытым: скрытое видеонаблюдение в учреждении не осуществляется.

## 2. Цели и правовые основания видеонаблюдения

2.1. Целями видеонаблюдения являются:

1) обеспечение безопасности воспитанников, работников и иных лиц, находящихся в здании и на территории учреждения;

2) обеспечение антитеррористической защищённости объекта (территории), в том числе контроль обстановки, пропускного и внутриобъектового режимов;

3) предупреждение и пресечение противоправных посягательств, установление обстоятельств происшествий, конфликтных ситуаций и несчастных случаев;

4) обеспечение сохранности имущества учреждения, воспитанников и работников;

5) осуществление контроля за соблюдением правил внутреннего распорядка в части, не связанной с постоянным контролем за исполнением трудовой функции работниками.

2.2. Правовыми основаниями обработки персональных данных с использованием системы видеонаблюдения являются пункт 2 части 1 статьи 6 Федерального закона № 152-ФЗ (обработка необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей, в том числе по обеспечению антитеррористической защищённости объекта и безопасности воспитанников) и пункт 7 части 1 статьи 6 Федерального закона № 152-ФЗ (обработка необходима для осуществления прав и законных интересов оператора при условии, что при этом не нарушаются права и свободы субъекта персональных данных).

2.3. Получение согласия субъектов персональных данных на обработку персональных данных с использованием системы видеонаблюдения не требуется. Учреждение обеспечивает информирование субъектов персональных данных о ведении видеонаблюдения в порядке, установленном разделом 5 настоящего Положения.

2.4. Видеонаблюдение не используется в целях, не предусмотренных пунктом 2.1 настоящего Положения, в том числе в целях постоянного контроля за выполнением работниками трудовой функции, сбора сведений о частной жизни, политических, религиозных и иных убеждениях, состоянии здоровья субъектов персональных данных.

## 3. Биометрические персональные данные: ограничение обработки

3.1. В системе видеонаблюдения учреждения биометрические персональные данные не обрабатываются.

3.2. В соответствии с частью 1 статьи 11 Федерального закона № 152-ФЗ биометрическими персональными данными являются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Видеоизображение, получаемое системой видеонаблюдения, не используется учреждением для установления личности на основании указанных особенностей, в связи с чем не относится к биометрическим персональным данным.

3.3. В системе видеонаблюдения запрещается:

1) применение программных и программно-аппаратных средств автоматического распознавания лиц, построения и хранения биометрических шаблонов (векторов) лиц, иной биометрической идентификации и аутентификации;

2) сопоставление видеоизображений с эталонными биометрическими образцами, в том числе с использованием внешних сервисов и информационных систем;

3) передача видеоизображений в единую биометрическую систему и иные информационные системы, осуществляющие обработку биометрических персональных данных;

4) использование функций видеоаналитики, обеспечивающих идентификацию конкретного физического лица.

3.4. Включение в состав системы видеонаблюдения оборудования или программного обеспечения, реализующего функции, указанные в пункте 3.3 настоящего Положения, допускается исключительно после внесения изменений в настоящее Положение, проведения оценки вреда, актуализации модели угроз безопасности информации и акта установления уровня защищённости, а также получения согласий субъектов персональных данных в письменной форме в соответствии с частью 1 статьи 11 Федерального закона № 152-ФЗ.

## 4. Состав, размещение и режим работы системы видеонаблюдения

4.1. Перечень мест размещения видеокамер и зон видеонаблюдения утверждается приказом заведующего учреждения и пересматривается при изменении состава оборудования, но не реже одного раза в год.

4.2. Видеокамеры не размещаются в туалетных и душевых комнатах, раздевалках, медицинском кабинете (за исключением входа в него), помещениях для отдыха и приёма пищи работников, а также в иных помещениях, видеонаблюдение в которых нарушало бы неприкосновенность частной жизни.

4.3. Система видеонаблюдения работает в режиме, установленном утверждённым перечнем видеокамер, без записи звука. Запись аудиоинформации (прослушивание) не осуществляется.

4.4. Оборудование хранения видеозаписей размещается в помещении, доступ в которое ограничен и входит в границы контролируемой зоны учреждения.

4.5. Техническое обслуживание системы видеонаблюдения осуществляется работником учреждения, ответственным за техническое обслуживание информационных систем, либо сторонней организацией на основании договора, содержащего условие о поручении обработки персональных данных и об обязанности соблюдать конфиденциальность (части 3, 5 статьи 6 Федерального закона № 152-ФЗ).

## 5. Информирование о ведении видеонаблюдения

5.1. Учреждение информирует субъектов персональных данных о ведении видеонаблюдения путём размещения информационных табличек (знаков) при входе на территорию, при входе в здание и в помещениях, оборудованных видеокамерами.

5.2. Форма информационной таблички утверждается приказом заведующего учреждения и содержит сведения об операторе, целях и правовых основаниях видеонаблюдения, сроке хранения видеозаписей, об отсутствии обработки биометрических персональных данных и способах обращения к оператору.

5.3. Настоящее Положение размещается на официальном сайте учреждения https://belsolnishkokrinichnoe.eduds.ru и на информационном стенде учреждения.

5.4. Работники учреждения уведомляются о ведении видеонаблюдения под подпись при приёме на работу, а работающие на день введения системы в эксплуатацию — в течение одного месяца со дня издания соответствующего приказа.

Родители (законные представители) воспитанников информируются о видеонаблюдении при приёме в образовательную организацию.

## 6. Хранение и уничтожение видеозаписей

6.1. Срок хранения видеозаписей составляет 7 календарных дней с момента их создания, если иной срок не установлен законодательством Российской Федерации или не требуется для достижения целей обработки.

6.2. По истечении срока хранения видеозаписи уничтожаются автоматически путём перезаписи (циклической записи) на носителе информации.

6.3. Срок хранения отдельной видеозаписи может быть продлён приказом заведующего учреждения в случае, если видеозапись относится к происшествию, несчастному случаю, конфликтной ситуации, дисциплинарному или административному производству, а также при поступлении запроса уполномоченного органа. Такие видеозаписи копируются на отдельный носитель и хранятся до разрешения соответствующего вопроса по существу, после чего уничтожаются с составлением акта.

6.4. Уничтожение (удаление) видеозаписей, скопированных на отдельные носители, осуществляется комиссией с составлением акта об уничтожении (удалении) видеозаписей по форме, утверждённой приказом заведующего учреждения.

6.5. Не допускается хранение видеозаписей на личных носителях информации работников, в личных учётных записях облачных сервисов и на оборудовании, не входящем в состав системы видеонаблюдения.

## 7. Порядок доступа к видеозаписям и их предоставления

7.1. Доступ к средствам просмотра и архиву видеозаписей предоставляется ограниченному кругу лиц, определённому приказом заведующего учреждения, и осуществляется в объёме, необходимом для выполнения должностных обязанностей.

7.2. Каждый случай доступа к архиву видеозаписей (просмотр, копирование, выдача) регистрируется в журнале учёта доступа к архиву системы видеонаблюдения и выдачи видеозаписей.

7.3. Видеозаписи предоставляются третьим лицам исключительно в случаях, предусмотренных законодательством Российской Федерации: по мотивированному запросу суда, органов прокуратуры, органов внутренних дел, органов федеральной службы безопасности, органов следствия и дознания, иных уполномоченных органов, оформленному в письменной форме с указанием правового основания, цели и объёма запрашиваемых сведений. Передача оформляется актом или сопроводительным письмом с регистрацией в журнале.

7.4. Субъект персональных данных вправе обратиться к оператору с запросом о наличии видеозаписей, содержащих его персональные данные, об ознакомлении с ними, а также об их уточнении, блокировании или уничтожении, если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки (статьи 14, 20, 21 Федерального закона № 152-ФЗ). Запрос рассматривается в порядке и сроки, установленные Правилами рассмотрения запросов субъектов персональных данных или их представителей.

7.5. При ознакомлении субъекта персональных данных с видеозаписью учреждение обеспечивает соблюдение прав иных лиц, попавших в кадр, в том числе путём демонстрации видеозаписи без её копирования и передачи.

7.6. Размещение видеозаписей и их фрагментов в информационно-телекоммуникационной сети «Интернет», в мессенджерах и социальных сетях не допускается.

## 8. Обязанности ответственного за эксплуатацию системы видеонаблюдения

8.1. Ответственный за эксплуатацию системы видеонаблюдения:

1) обеспечивает работоспособность системы видеонаблюдения и соответствие фактического размещения видеокамер утверждённому перечню;

2) обеспечивает ограничение доступа к средствам просмотра и архиву видеозаписей;

3) ведёт журнал учёта доступа к архиву системы видеонаблюдения и выдачи видеозаписей;

4) контролирует соблюдение сроков хранения и организует уничтожение (удаление) видеозаписей;

5) обеспечивает размещение и сохранность информационных табличек;

6) незамедлительно информирует ответственного за организацию обработки персональных данных о выявленных инцидентах информационной безопасности;

7) не реже одного раза в квартал проводит проверку работоспособности системы и корректности настроек, исключающих применение функций биометрической идентификации.

## 9. Меры по обеспечению безопасности персональных данных

9.1. Информационной системе персональных данных «Видеонаблюдение» установлен 4 уровень защищённости. Категории данных: иные. Категории субъектов: работники; воспитанники; родители (законные представители); посетители. Количество субъектов: менее 100 тыс. Тип актуальных угроз: 3.

9.2. Для обеспечения установленного уровня защищённости в учреждении реализуются:

1) режим обеспечения безопасности помещений, в которых размещены оборудование хранения видеозаписей и средства просмотра, препятствующий возможности неконтролируемого проникновения или пребывания в них посторонних лиц;

2) обеспечение сохранности носителей персональных данных;

3) утверждение перечня лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей;

4) применение средств защиты информации, прошедших процедуру оценки соответствия в форме, определяемой оператором самостоятельно (пункт 6 Состава и содержания мер, утверждённых приказом ФСТЭК России от 18 февраля 2013 г. № 21), включая парольную защиту, разграничение прав доступа, регистрацию событий и антивирусную защиту.

9.3. Применяемые средства защиты видеоинформации и обоснование соответствия актуальным угрозам: система видеонаблюдения не подключена к сети «Интернет», удалённый доступ отсутствует; видеорегистратор размещён в запираемом помещении детского сада с ограниченным доступом.

9.4. Требования к применению сертифицированных средств защиты определяются с учётом статуса информационной системы, установленного уровня защищённости и актуальных угроз безопасности персональных данных. Обоснование выбранных средств защиты фиксируется в документах по защите информационной системы.

9.5. В случае выявления инцидента информационной безопасности, повлекшего неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, учреждение действует в соответствии с Положением по работе с инцидентами информационной безопасности и частью 3.1 статьи 21 Федерального закона № 152-ФЗ, уведомляя

уполномоченный орган по защите прав субъектов персональных данных в течение 24 часов и о результатах внутреннего расследования — в течение 72 часов.

## 10. Ответственность

10.1. Лица, допущенные к работе с системой видеонаблюдения, несут дисциплинарную, материальную, административную и уголовную ответственность, предусмотренную законодательством Российской Федерации, за нарушение порядка обработки персональных данных, разглашение сведений, ставших им известными в связи с работой с системой видеонаблюдения, в том числе в соответствии со статьёй 13.11 Кодекса Российской Федерации об административных правонарушениях и статьёй 137 Уголовного кодекса Российской Федерации.

10.2. Контроль за соблюдением настоящего Положения осуществляет ответственный за организацию обработки персональных данных.

## 11. Заключительные положения

11.1. Настоящее Положение вступает в силу со дня его утверждения приказом заведующего учреждения и действует до его отмены или замены новым.

11.2. Изменения в настоящее Положение вносятся приказом заведующего учреждения в случае изменения законодательства Российской Федерации, состава и конфигурации системы видеонаблюдения, целей обработки персональных данных.

Заведующий Любимова Н.Н.