

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ
Г.ХАБАРОВСКА «ВОЛОЧАЕВСКИЙ ЛИЦЕЙ»**

ПРИНЯТО
педагогическим советом
« 12 » января 2024г.
протокол № 5

УТВЕРЖДЕНО
Приказом № 11
От 12.01.2024
Директор МБОУ
«Волочаевский лицей»

С.В. Якушенко

ПОЛОЖЕНИЕ
о системе видеонаблюдения в МБОУ
«Волочаевский лицей»

1. ОБЩИЕ ПОЛОЖЕНИЯ

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 12.02.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», 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».

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

С целью противодействия терроризму и совершению противоправных действий, МБОУ «Волочаевский лицей» обязано вести видеонаблюдение за состоянием обстановки в режиме реального времени на всех своих территориях и помещениях, архивировать и хранить данные в течение 30 суток.

Система видеонаблюдения (далее – СВН) в МБОУ «Волочаевский лицей» необходима для защиты (безопасности) персонала, обучающихся 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 образовательного процесса.

СВН является открытой, направлена на контроль дисциплины сотрудников, а также обучающихся и порядка в образовательном учреждении, предупреждения возникновения чрезвычайных ситуаций и обеспечения сохранности имущества.

Настоящее Положение обязательно для работников, обучающихся и (или) посетителей МБОУ «Волочаевский лицей». Настоящее Положение подлежит размещению на официальном сайте и находится в свободном доступе

для работников, обучающихся и (или) посетителей МБОУ «Волочаевский лицей».

2. ПОРЯДОК ОРГАНИЗАЦИИ СВН

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

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

Лица, являющиеся сотрудниками образовательного учреждения на момент введения СВН, должны в письменной форме выразить свое согласие или несогласие на введение данной системы (заполнение согласия на обработку персональных данных). Если работник не согласен на изменение условий трудового договора, то после выполнения процедур, предусмотренных Трудовым кодексом РФ трудовой договор с ним может быть расторгнут по пункту 7 статьи 77 ТК РФ.

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

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

Места установки видеокамер в образовательном учреждении определяются по мере необходимости в соответствии с конкретными задачами решением директора.

Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры), а также в помещениях, где осуществляется образовательная деятельность.

Установка видеокамер не допускается в туалетных, душевых комнатах и в комнатах для переодевания работников и обучающихся.

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

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

3. ЦЕЛИ И ЗАДАЧИ СВН

Целью СВН является создание условий для антитеррористической защищенности в учреждении, безопасности персонала и обучающихся, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, осуществление внутреннего контроля качества и безопасности образовательной деятельности.

Задачами организации видеонаблюдения являются:

- контроль за обстановкой на территориях и в помещениях 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, обучающихся и посетителей;
- установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником, обучающимся, 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, обучающихся и посетителей учреждения;
- охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а также предупреждение случаев хищения имущества учреждения и/или работников/обучающихся/посетителей;
- отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;
- информационное обеспечение принятия решений директором;
- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

СВН должна обеспечивать:

- видеофиксацию 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.

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)

Образовательное 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

СВН предполагает запись информации в режиме реального времени на сервер, 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 образовательных услуг, уничтожается автоматически по мере заполнения памяти жесткого диска до 30 суток.

Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с сервера.

Исключение составляют случаи официального письменного обращения с разрешения директора образовательного учреждения.

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

- в помещение охраны/вахты с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;

- в кабинете заместителя директора по УВР (в корпусе № 1)

Разрешение доступа к просмотру записей видеонаблюдения, хранящихся установленный период на жестком диске сервера, осуществляется:

- для просмотров записей в классах и коридорах с разрешения заместителя директора по безопасности, директора образовательного учреждения;

- для просмотров записей, установленных для антитеррористической защищенности учреждения, с разрешения директора учреждения.

На основании письменного разрешения директора 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.

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

Генерация и выдача паролей доступа осуществляется ответственным за организацию работы СВН, назначенным приказом директора посредством ведения «Журнала генерации, учета и выдачи паролей доступа» под личную роспись. Смена пароля или его продление осуществляется не реже одного раза в шесть месяцев (либо при увольнении этих должностных лиц).

Просмотр записанных изображений может осуществляться исключительно при личном участии должностных лиц, имеющих право на просмотр видеоматериалов.

Для защиты публичных интересов (т.е. выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи

и сотрудники полиции (и сотрудники других правоохранительных органов РФ).

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).

Решение о передаче записей принимает директор или заместитель директора по безопасности.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

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.

Работникам учреждения (кроме уполномоченных на то лиц) и охранной организации **ЗАПРЕЩАЕТСЯ:**

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

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

7. ОРГАНИЗАЦИЯ ВСЕСТОРОННЕГО ОБЕСПЕЧЕНИЯ РАБОТЫ СВН.

Ответственность за проведение технического обслуживания, в том числе проведения ремонтных работ для поддержания работоспособности СВН возлагается на заместителя директора по безопасности и заместителя директора по АХР.

Ответственность за работоспособность программно-аппаратного комплекса СВН, в том числе его модернизацию (обновление операционных систем, САВЗ, системы разграничения доступа и т.д.) возлагается на обслуживающую организацию.

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 с записью в журнале учета вскрытия помещений (приложение 2).

Ответственность за предотвращение неправомерного доступа к защищаемой информации, хранящейся на магнитных накопителях, контроль за ее использованием, возлагается на ответственного за организацию работы СВН

по защите информации.

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 с записью в журнале учета вскрытия помещения, приложение 2;

- обеспечением хранения и выдачи ключей от помещений, где используются магнитные накопители СВН с записью в журнале учета и выдачи ключей, приложение 3;

- учетом магнитных носителей информации используемых в СВН в «Журнале учета СКЗИ МИО АСУ».

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

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

Ознакомление сотрудников учреждения с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под роспись.

Один экземпляр настоящего положения выдается под роспись директору (руководителю) охранной организации (предприятия) с которой заключен действующий Контракт на оказание охранных услуг.