

**Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение «Колледж «Звёздный»**

ПРИНЯТ
Педагогическим советом
СПб ГБ ПОУ
«Колледж «Звёздный»
Протокол от «17» 06 2022 года № 10

УТВЕРЖДЕН
Приказом СПб ГБ ПОУ
«Колледж «Звёздный»
от «17» 06 2022 года № 61-О

ЛОКАЛЬНЫЙ АКТ № 117

**Положение о системе видеонаблюдения
Санкт-Петербургского государственного бюджетного профессионального
образовательного учреждения «Колледж «Звёздный»**

X Документ подписан электр...

Пантелеенко Римма Александровна
Директор
Подписано: Пантелеенко Римма Александровна

1. Термины, определения и сокращения

1.1. Администратор ИБ ИСПДн (Администратор ИБ) – назначенный приказом работник, который согласно своей инструкции отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах эксплуатации и модернизации.

1.2. Информационная система (ИС) – совокупность содержащейся в базах информации и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей СПб ГБ ПОУ "Колледж "Звездный", а также транспортных средств.

1.4. Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

1.5. Защищаемая информация (ЗИ) – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативно-правовых документов.

2. Общие положения

2.1. Настоящее положение разработано в соответствии с Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ, Федеральным законом от 27.07.2006 № 149-Ф «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

2.2. 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.

2.3. Система открытого видеонаблюдения в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении "Колледж "Звездный"(далее - СПб ГБ ПОУ "Колледж "Звездный") является элементом общей системы безопасности образовательного учреждения, направленной на обеспечение безопасности рабочего процесса, поддержание трудовой дисциплины и порядка, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.

2.4. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности работников СПб ГБ ПОУ "Колледж "Звездный" и не может быть направлена на сбор информации о конкретном человеке.

3. Цели и задачи системы видеонаблюдения

Система видеонаблюдения призвана выполнять следующие задачи:

3.1. повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций;

3.2. обеспечение противопожарной защиты зданий и сооружений;

3.3.обеспечение антитеррористической защиты работников и территории СПб ГБ ПОУ "Колледж "Звездный", охраны порядка и безопасности;

3.4. совершенствование системы информирования и оповещения работников СПб ГБ ПОУ "Колледж "Звездный" об угрозе возникновения кризисных ситуаций;

3.5. пресечение противоправных действий со стороны работников СПб ГБ ПОУ "Колледж "Звездный" и посетителей.

Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. 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 лица, совершившего соответствующее противоправное действие.

4. Порядок организации системы видеонаблюдения

4.1. Решение об установке системы видеонаблюдения принимается директором СПб ГБ ПОУ "Колледж "Звездный" .

4.2. Система видеонаблюдения входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.

4.3. Система видеонаблюдения выполняет следующие функции:

4.3.1. визуальное наблюдение за контролируемой территорией и ее периметром;

4.3.2. запись архива.

4.4. Установка системы видеонаблюдения осуществляется в соответствии с ее целями и задачами согласно проектной документации:

4.4.1. в местах возможного несанкционированного проникновения посторонних лиц (входные зоны);

4.4.2. в местах повышенного риска возникновения опасных ситуаций: коридорах, вестибюле первого этажа, столовой, спортивных залах, библиотека- у нет;

4.4.3. по периметру здания на улице.

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

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

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

4.8. При обнаружении нарушения правил эксплуатации системы видеонаблюдения, обнаруживший нарушение работник оповещает о факте нарушения заместителю директора по АХЧ и(или) директору, приняв соответствующие меры по приостановке эксплуатации системы видеонаблюдения.

5. Меры по обеспечению безопасности данных

5.1. Отображения процесса видеозаписи производиться на экране монитора, расположение которого исключает его просмотр сторонними лицами. Для помещения, в которых располагаются мониторы. организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации.

5.2. Программное обеспечение, позволяющее просматривать видеозаписи с видеорегистраторов, должно быть защищено паролем доступа. Приказом директора назначается ответственный за ограничение доступа к видеозаписям. С целью решения вопросов технического обслуживания оборудования заключается договор со специализированной организацией, имеющей лицензию на выполнение данного вида работ.

5.3. Система видеонаблюдения работает в круглосуточном режиме. Видеозапись осуществляется на видеорегистраторах, входящих в состав установленной на объекте системы видеонаблюдения. Уничтожение видеозаписей производиться 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.

5.4. В тех случаях, когда система видеонаблюдения позволяет отслеживать

деятельность работников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой ЗИ.

5.2. Обработка ЗИ в СПб ГБ ПОУ "Колледж "Звездный" регламентируется внутренней организационно-распорядительной документацией в соответствии с приказом об утверждении документов по информационной безопасности от 13 апреля 2022 г.

5.3. СПб ГБ ПОУ "Колледж "Звездный" обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ, и принятыми в соответствии с ним нормативными правовыми актами.

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

5.5. Хранение ЗИ должно осуществляться не дольше, чем этого требуют цели обработки ЗИ в соответствии с законодательством.

5.6. Обработываемая ЗИ подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

6. Ответственность за нарушение правил обработки данных

6.1. Персональную ответственность за организацию и контроль использования носителей ЗИ несет Администратор ИБ.

6.2. Персональную ответственность за сохранность носителей ЗИ и предотвращение несанкционированного доступа к записанной на них информации несут работники, получившие эти носители.

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

6.4. В случае утери или уничтожения носителя информации ответственный Администратор ИБ немедленно ставит об этом в известность СПб ГБ ПОУ "Колледж "Звездный".

6.5. Установление причин и обстоятельств утери или уничтожения носителя информации возлагается на лицо, назначенное ответственным за обеспечение ИБ. Все работники обязаны оказывать содействие и не создавать препятствий в проведении проверки указанных причин и обстоятельств.

6.6. Информация о результатах установления причин и обстоятельств нарушений Положения, должна быть оформлена и предоставлена ответственному лицу не позднее 10 дней со дня обнаружения факта утери или уничтожения носителя информации.

6.7. За утерю или уничтожение носителя информации, работник может быть привлечен к дисциплинарной и иной предусмотренной законодательством РФ ответственности.

6.8. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами ИСПДн, обрабатывающими информацию ограниченного доступа, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством РФ ответственности.

6.9. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ЗИ, должны соблюдаться следующие условия:

6.9.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ЗИ, осуществляемой без использования средств автоматизации,

наименование и адрес оператора, фамилию, имя, отчество и адрес субъекта ЗИ, источник получения ЗИ, сроки обработки, перечень действий с ЗИ, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ЗИ;

6.9.2. типовая форма должна предусматривать поле, в котором субъект ЗИ может поставить отметку о своем согласии на обработку ЗИ, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ЗИ;

6.9.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ЗИ, содержащихся в документе, имел возможность ознакомиться со своими ЗИ, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ЗИ;

6.9.4. типовая форма должна исключать объединение полей, предназначенных для внесения ЗИ, цели обработки которых заведомо не совместимы.

6.10. Уточнение ЗИ при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на бумажном носителе, либо путем изготовления нового бумажного носителя с уточненными ЗИ.

7. Уничтожение информации, содержащейся на бумажных носителях ЗИ

7.1. Уничтожение или обезличивание части ЗИ, производится способом, исключающим дальнейшую обработку этих ЗИ с сохранением возможности обработки иных данных, зафиксированных на бумажном носителе (удаление, вымарывание). Указанные правила, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном бумажном носителе ЗИ и информации, не являющейся ЗИ.

8. Меры по обеспечению безопасности информации, содержащейся на бумажных носителях ЗИ

8.1. При хранении материальных носителей ЗИ должны соблюдаться условия, обеспечивающие сохранность ЗИ и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются образовательным учреждением.

8.2. Обработка ЗИ, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ЗИ можно было определить места хранения ЗИ (материальных носителей) и установить перечень лиц, осуществляющих обработку ЗИ либо имеющих к ним доступ.

9. Контроль материальных носителей ЗИ

9.1. Проверка наличия носителей ЗИ осуществляется Администратором ИБ в соответствии с должностной инструкцией.

10. Ответственность

10.1. Персональную ответственность за организацию и контроль использования носителей ЗИ несет Администратор ИБ.

10.2. Персональную ответственность за сохранность носителей ЗИ и предотвращение несанкционированного доступа к записанной на них информации несут работники, получившие эти носители.

10.3. Работники, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством РФ ответственность.

10.4. В случае утери или уничтожения носителя информации руководитель структурного подразделения немедленно ставит об этом в известность ответственного за обработку.

10.5. Установление причин и обстоятельств утери или уничтожения носителя информации возлагается на Администратора ИБ. Все работники образовательного учреждения обязаны оказывать содействие и не создавать препятствий в проведении проверки указанных причин и обстоятельств.

10.6. Информация о результатах установления причин и обстоятельств нарушений Положения, должна быть оформлена и предоставлена Ответственному за обработку не позднее 10 дней со дня обнаружения факта утери или уничтожения носителя информации.

10.7. За утерю или уничтожение носителя информации, работник может быть привлечен к дисциплинарной и иной предусмотренной законодательством РФ ответственности.

10.8. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами ИСПДн, обрабатывающими информацию ограниченного доступа, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством РФ ответственности.