Приложение №1 к Приказу
№ 590 от «07» 11 2024 г.

ПОЛОЖЕНИЕ
о применении системы аудио-видеонаблюдения в федеральном государственном бюджетном образовательном учреждении высшего образования «Херсонский технический университет»

1. Общие положения

1.1. Настоящее Положение о системе видеонаблюдения (далее — Положение) в федеральном государственном бюджетном образовательном учреждении высшего образования «Херсонский технический университет», (далее — Университет) разработано в соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ), Федеральным законом от 06.03.2006 №35-ФЗ «О противодействии терроризму», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, постановлением Правительства Российской Федерации от 7 ноября 2019 года № 1421 « Об утверждении требований к антитеррористической защищенности объектов (территорий) министерства науки и высшего образования Российской Федерации и подведомственным ему организаций объектов (территорий) относящихся к сфере деятельности науки и высшего образования Российской Федерации» уставом Университета, Правилами внутреннего трудового распорядка ФГБОУ ВО «ХТУ» и иными локальными нормативными актами Университета.

1.2. Настоящее Положение устанавливает порядок осуществления аудио-видео наблюдения на территории и в зданиях Университета, цели и способы его осуществления, порядок доступа к аудио-видеоматериалам, их хранения и уничтожения, порядок передачи и использования аудио-видеоматериалов.

1.3. Система аудио-видеонаблюдения в Университете является элементом общей системы безопасности Университета, гарантирующей постоянный контроль над охраняемой зоной в целях обеспечения общественной безопасности, направленной на предупреждение возможных террористических, экстремистских акций и других противоправных и криминальных проявлений в отношении абитуриентов, обучающихся, работников и посетителей Университета, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования в случаях их возникновения.

1.4. Система аудио-видеонаблюдения в Университете является открытой, создана и функционирует с использованием камер открытого наблюдения для решения следующих задач:

- отслеживание, фиксация, своевременная передача изображений и данных объектов в целях создания условий для обеспечения безопасности, недопущения ущерба жизни и здоровью работников, абитуриентов, обучающихся и посетителей Университета, а также убытков Университета, минимизации материального ущерба в условиях действия дестабилизирующих факторов;
- защита участников образовательного процесса, их прав и интересов, имущества от неблагоприятных воздействий;
- раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;
- информационная поддержка принятия решений органами управления Университета;

- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством;
- обеспечение безопасности образовательного процесса, своевременного реагирования при возникновении опасных ситуаций, принятие необходимых мер по оказанию помощи и защите работников, абитуриентов, обучающихся и посетителей Университета в случае чрезвычайного происшествия;
- обеспечение контрольно-пропускного режима, контроля и управления доступом и соблюдения Правил внутреннего трудового распорядка Университета;
- контроль за обстановкой, в том числе во внутренних помещениях и в пределах территории Университета, обеспечивающий защиту от несанкционированного проникновения на территорию посторонних лиц и транспортных средств;
- повышение эффективности действий сотрудников охраны при возникновении нештатных и чрезвычайных ситуаций, их предотвращение и устранение;

1.5. Система аудио-видеонаблюдения не направлена на сбор информации о конкретном субъекте персональных данных.

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

1.7. Аудио-видеонаблюдение за объектами, имеющими режим ограниченного доступа, не ведется.

1.8. Настоящее Положение обязательно для всех участников образовательного процесса.

2. Основные понятия и сокращения

2.1. Под аудио-видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеофиксации об объекте и помещениях, а также запись полученного изображения и его хранение для последующего использования.

2.2. Система видеонаблюдения (video surveillance system, VSS) - совокупность функционирующих видеоканалов, программных и технических средств записи и хранения видеоданных, а также программных и технических средств управления, осуществляющих информационный обмен между собой;

2.3. Видеокамера (camera) - техническое средство, предназначенное для преобразования оптического изображения в телевизионные видеоданные;

2.4. Видеосервер, видеорегистратор (video server) - устройство, предназначенное для приема и хранения аудио-видеоданных с видеокамер, а также удаленного воспроизведения с помощью программного обеспечения

2.5. Несанкционированные действия (НСД) - преднамеренные действия, направленные на нарушение правильности функционировании системы;

2.6. Посетители — гости Университета, сотрудники сторонних организаций (приглашенные, прикомандированные, выполняющие обязательства по гражданско-правовым договорам, заключенным с Университетом);

2.7. Объекты Университета — административные здания, учебные, учебно-лабораторные корпуса, в том числе гаражи, внутренняя территория Университета, студенческих городков, ФГБОУ ВО «ХТУ».

3. Требования к системе аудио-видеонаблюдения

3.1. Система видеонаблюдения должна обеспечивать:

- видеоверификацию тревог (подтверждение обнаружения проникновения) - подтверждение с помощью аудио-видеонаблюдения факта несанкционированного проникновения в зоне охраны и выявление ложных срабатываний;
- прямое видеонаблюдение сотрудником отдела контроля доступа управления комплексной безопасности университета, а также охранником Частной охранной организации в зоне охраны;

- запись аудио-видеоинформации в архив не менее 30 суток для последующего анализа состояния охраняемого объекта (зоны), тревожных ситуаций, идентификации нарушителей и других задач;
- прогнозирование и предупреждение противоправных действий на объектах, аварийных ситуаций;
- непрерывность сбора, передачи и обработки информации;
- разграничение полномочий доступа к управлению и видеоинформации с целью предотвращения несанкционированных действий;
- воспроизведение ранее записанной информации;
- оперативный доступ к видеозаписи и видеоархиву путем задания времени, даты и идентификатора телекамеры.
- обеспечение противопожарной защиты объектов университета, антитеррористической защиты работников, обучающихся, посетителей и территорий университета.

3.2. Система аудио-видеонаблюдения должна обеспечивать контроль следующих основных дестабилизирующих факторов (параметры контроля):
- незаконного проникновения посторонних лиц, животных или чужеродных предметов, аппаратов, тел на объекты;
- антропогенного, физического, химического, электромагнитного воздействия на сами видеокамеры или на объекты;
- возникновения пожара;
- нарушения в подаче электроэнергии;
- несанкционированного проникновения в служебные помещения;
- затопления помещений, дренажных систем и технологических приямков;
- изменения состояния основания, строительных (инженерно-технических) конструкций зданий и сооружений;
- нарушения работоспособности систем противоаварийной защиты, безопасности и противопожарной защиты;
- сооружений инженерной защиты;

4.Описание системы аудио-видеонаблюдения

4.1. Система представляет собой программно-аппаратный комплекс, не входящий в перечень специальных технических средств, предназначенных для негласного получения информации, включающий:
- камеры видеонаблюдения;
- видеомониторы;
- источники бесперебойного питания;
- видеорегистраторы и видеосерверы;
- сетевая (кабельная) инфраструктура;
- средства хранения видеоинформации;
- программное обеспечение для просмотра изображений.

4.2. Зоны установки камер наблюдения:
- в местах возможного несанкционированного проникновения посторонних лиц (центральных входах, запасных выходах), по периметру зданий Университета;
- в коридорах;
- на лестничных пролетах;
- на входных группах и на этажах общежитий;
- в помещениях для занятия спортом и проведения досуговых мероприятий;
- в фойе;
- в учебных аудиториях и компьютерных классах;
- в помещениях постоянного хранения материальных ценностей;
- в научно-исследовательских лабораториях;

- в серверных помещениях;
- в актовых и кинозалах;
- на удаленных постах;
- на контрольно-транспортном пункте;
- в местах расположения турникетов на входных группах;
- по периметру ограждений.

4.3. Режим видеонаблюдения:

- система функционирует 24 часа в сутки, 7 дней в неделю, в том числе в выходные и нерабочие праздничные дни;

4.4. Отображение процесса видеонаблюдения производится на мониторах, установленных в отделе контроля доступа УКБ университета и стационарных постах охраны, с целью своевременного реагирования при появлении признаков опасной ситуации.

4.5. В процессе аудио-видеонаблюдения производится запись видеоинформации на материальные носители (жёсткие диски) специализированных видеосерверов и видеорегистраторов.

4.6. Срок хранения записей составляет не менее 30 дней, после этого срока записи автоматически уничтожаются. Если камеры видеонаблюдения зафиксировали конфликтную (нестандартную) ситуацию, то для таких записей указанием начальником Управления комплексной безопасности устанавливается специальный срок хранения до 3 лет.

5 Порядок организации видеонаблюдения

5.1. Аудио-видеонаблюдение в Университете осуществляется постоянно с передачей видеоизображения в режиме реального времени и синхронизацией событий с системой единого точного времени.

5.2. Администрирование системы видеонаблюдения осуществляет отдел инженерно-технического обеспечения Управления комплексной безопасности.

5.3. Техническое сопровождение системы видеонаблюдения и информационная безопасность видеоматериалов обеспечивается Управлением комплексной безопасности.

5.4. Работники, принимаемые на работу лица, обучающиеся и поступающие в Университет, которые потенциально могут попасть в зону работы камер видеонаблюдения, информируются об этом в следующих формах:

- размещение специальных объявлений и/или общепринятых предупредительных знаков (табличек) перед входом на территорию, на которой ведется видеонаблюдение, в учебных аудиториях, компьютерных классах, спортивных и актовых залах;
- информирование участников образовательного процесса на общих собраниях;
- ознакомление с данным Положением участников образовательного процесса университета путем размещения в личном кабинете обучающегося и на официальном сайте Университета;
- иные способы, позволяющие гражданину принять решение о том, готов ли он стать объектом видеонаблюдения.

5.5. Использование изображений субъектов персональных данных, зафиксированных камерами наблюдения, осуществляется в строгом соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Порядок доступа к видеоматериалам и передача третьим лицам

6.1. Информация, записываемая системой видеонаблюдения, является конфиденциальной, не подлежит перезаписи с жестких дисков специализированных видеосерверов, редактированию и передаче третьим лицам.

6.2. Вся записываемая видеоинформация может быть использована только в соответствии с действующим законодательством Российской Федерации и настоящим Положением.

6.3. Доступ к видеоинформации, хранящейся на жестких дисках специализированных видеосерверов, может осуществляться только по локальной сети системы видеонаблюдения Университета. Видеоматериалы не могут выкладываться в сети Интернет.

6.4. Допуск к просмотру видеоматериалов, хранящихся на жёстких дисках специализированных видеосерверов и видеорегистраторов, а также видеоматериалов с камер, фиксирующих проходы через систему контроля и управления доступом имеют ректор, работники управления комплексной безопасности.

6.5. Просмотр необходимых видеоматериалов может осуществляться иными работниками по согласованию с начальником управления комплексной безопасности. К просмотру могут также привлекаться должностные лица Университета (в части их касающейся), а также обучающиеся и работники Университета, работники службы охраны, имеющие отношение к событиям, зафиксированным системой видеонаблюдения. Для защиты публичных интересов (т. е. выявления факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, либо их родители (законные представители) и сотрудники правоохранительных органов.

6.6. Передача видеоматериалов третьей стороне допускается только по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством. Вопрос о передаче материалов решает начальник управления комплексной безопасности. Передача видеоматериалов осуществляется отделом технической поддержки управления цифровых технологий, отделом контроля доступа управления комплексной безопасности, выполняющим функции администратора системы видеонаблюдения.

7. Безопасность персональных данных

7.1. Информация, собранная на видеомонитор при помощи системы видеонаблюдения, относится к персональным данным, за разглашение которых виновные лица могут быть привлечены к дисциплинарной ответственности.

7.2. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность работников Университета на рабочем месте, такое наблюдение будет считаться обработкой персональных данных.

7.3. Университет обязуется принимать меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативно-правовых актов.

8. Порядок введения системы видеонаблюдения

8.1. Система аудио-видеонаблюдения вводится в университете на основании приказа ректора.

8.2. Ответственным лицом за внедрение, организацию работы и контроль за работой системы видеонаблюдения является начальник управления комплексной безопасности Университета.

9. Ответственность

9.1. Лица, виновные в причинении вреда субъектам персональных данных, нарушением конфиденциальности записей камер видеонаблюдения, несут ответственность в порядке, предусмотренном законодательством Российской Федерации.

10. Заключительные положения

10.1. Настоящее Положение вводится в действие со дня утверждения приказом ректора Университета.

10.2. Изменения и дополнения в настоящее положения вносятся приказом ректора.

Разработал
Начальник отдела КД УКБ Н.В. Шишенко

Приложение №2 к Приказу
№ 590 от «07» 11 2024 г.

ЗАЯВЛЕНИЕ
о согласии на осуществление аудио-видеонаблюдения
на рабочем месте

Я, _____
(фамилия, имя, отчество)
занимающий должность:_____
_____,
с Приказом и положением ФГБОУ ВО «Херсонский технический университет» № 590 от «07» 11 2024г. «Об утверждении положения о системе аудио-видеонаблюдения в университете» ознакомлен(а). Даю свое согласие на осуществление видеонаблюдения на рабочем месте, а именно:

- осуществление видеонаблюдения и аудио записи на территории и в помещениях университета;

- использование Работодателем системы видеонаблюдения и аудио записи в целях обеспечения безопасности сторон трудового договора, контроля выполнения работниками Правил внутреннего трудового распорядка, обеспечения сохранности имущества, выявления нарушений законодательства Российской Федерации и локальных нормативных актов Работодателя;

- последующее хранение записей видеосъемки и аудио в соответствии с локальными нормативными актами Работодателя.

Настоящее согласие на аудио-видеосъемку действует с момента подписания трудового договора и может быть отозвано мной при представлении Работодателю заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации ч. 1 ст. 24 Конституции Российской Федерации, (сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются).

«___»_____ 20_____ г. _____ /_____
(подпись) (Ф.И.О.)