



Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ТюмГУ)

ПРИКАЗ

06.03.2019

г. Тюмень

№

264-1

Об утверждении Положения
о системе контроля и управления
доступом в ТюмГУ

В целях обеспечения комплексной безопасности ФГАОУ ВО «Тюменский государственный университет»

ПРИКАЗЫВАЮ:

1. Утвердить Положение о системе контроля и управления доступом в ФГАОУ ВО «Тюменский государственный университет» (далее – Положение) (Приложение).

2. Кухтериной Е.А., начальнику управления по работе с персоналом, в срок не позднее 15.03.2019 ознакомить под подпись работников университета с Положением; знакомить новых работников при трудоустройстве.

3. Директорам институтов, филиалов, школ, гимназии ТюмГУ, начальнику отдела аспирантуры и докторантуры в срок не позднее 15.03.2019 ознакомить под подпись обучающихся ТюмГУ с Положением; знакомить новых обучающихся при зачислении.

4. Исаки В.И., ведущему специалисту по обеспечению пропускного режима службы главного инженера, в срок не позднее 15.03.2019 ознакомить руководителя охранной организации и работников охраны с Положением.

5. Контроль исполнения приказа оставляю за собой.

Ректор

В.Н. Фальков

ПОЛОЖЕНИЕ
О СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
в федеральном государственном автономном образовательном учреждении
высшего образования «Тюменский государственный университет»

1. Термины и определения

В настоящем Положении применены термины, определяемые в Политике обеспечения информационной безопасности ФГАОУ ВО «Тюменский государственный университет» (далее – университет), а также:

1.1. Доступ – перемещение людей (субъектов доступа) и транспорта (объектов доступа) в помещения, здания, зоны и на территорию университета.

1.2. Уровень доступа – совокупность временных интервалов доступа и точек доступа, которые назначаются определенному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временные интервалы.

1.3. Зона доступа, зона – совокупность помещений университета, вход в которые оборудован единым комплексом средств контроля и управления доступом.

1.4. Контроль и управление доступом – комплекс мероприятий, направленных на предотвращения несанкционированного доступа.

1.5. Средства контроля и управления доступом – механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

1.6. Система контроля и управления доступом (далее – СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

1.7. Несанкционированный доступ – доступ субъектов доступа или объектов доступа, не имеющих права доступа.

1.8. Программное обеспечение (далее – ПО) – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

1.9. Идентификатор – уникальный признак субъекта или объекта доступа.

1.10. Карта доступа – идентификатор в виде физического носителя (карты), на который с помощью специальной технологии занесен идентификационный признак в виде кодовой информации.

1.11. Персонифицированная карта доступа – идентификатор в виде физического носителя (карты), на который с помощью специальной технологии занесен идентификационный признак в виде кодовой информации и нанесены персональные данные пользователя СКУД.

1.12. Пользователь СКУД – субъект доступа, в отношении которого осуществляются мероприятия по контролю доступа.

1.13. Оператор выдачи карт – подразделение университета, ответственное за выдачу, замену, блокировку и изъятие карт доступа пользователей СКУД.

1.14. GSM-идентификация – идентификация пользователя СКУД посредством звонка с сотового телефона, принадлежащего пользователю СКУД и внесенного в базу, на выделенный номер телефона с целью открытия шлагбаума или ворот.

2. Общие положения

2.1. Настоящее Положение определяет требования к организации контроля и управления доступом, описывает принципы и порядок функционирования системы контроля и управления доступом в университете.

2.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации,

информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными федеральными законами, уставом университета, Политикой обеспечения информационной безопасности в университете.

2.3. Настоящее Положение расширяет и уточняет требования Политики обеспечения информационной безопасности в университете и является ее неотъемлемой частью.

3. Система контроля и управления доступом

3.1. Система контроля и управления доступом предназначена для предотвращения несанкционированного доступа на территорию, в здания и помещения университета, обеспечения безопасности работников, обучающихся и посетителей, сохранности материальных и информационных ресурсов университета.

3.2. СКУД позволяет осуществлять:

- контроль перемещений работников, обучающихся и посетителей по университету;
- табельный учет рабочего времени работников;
- фиксацию времени прихода и ухода посетителей;
- временной и персональный контроль открытия помещений;
- совместную работу с системами охранно-пожарной сигнализации и видеонаблюдения;
- регистрацию информации о попытках осуществления несанкционированного доступа.

3.3. СКУД состоит из преграждающих управляемых устройств (турникеты, триподы, двери, оборудованные электромеханическими или электромагнитными замками, шлагбаумы), исполнительных устройств (идентификаторов, считывающих устройств (считывателей)), средств управления.

3.4. Средства управления СКУД включают в себя сервис, выполняющий следующие роли:

- объединение всех преграждающих управляемых устройств, средств управления и исполнительных устройств в единую информационную систему;
- взаимодействие с иными информационными системами университета, позволяющими идентифицировать субъекты доступа.

Описание информационных систем, используемых в средствах управления СКУД, их взаимодействия, ответственность подразделений университета за обеспечение их работоспособности утверждаются приказом по университету.

3.5. Основной вход в здания оборудован турникетами и контрольно-пропускными пунктами. Дополнительные входы в здания могут быть оборудованы турникетами, дверями с электромеханическими или электромагнитными замками.

3.6. Въезд на территорию университета оборудован шлагбаумами или воротами.

3.7. Вход в отдельные зоны и помещения может быть оборудован турникетами, дверями с электромеханическими или электромагнитными замками.

4. Карты доступа

4.1. Карта доступа представляет из себя электронный идентификатор беспроводного типа (Приложение)

4.2. Карты доступа подразделяются на постоянные и временные:

- постоянные карты доступа выдаются работникам и обучающимся и действуют с момента трудоустройства (зачисления) до момента увольнения (отчисления);
- временные карты доступа выдаются лицам, находящимся в договорных отношениях с университетом или являющимся работниками организаций,

находящихся в договорных отношениях с университетом, стажерам и практикантам и действуют в сроки, предусмотренные договором.

4.3. Выдача карт доступа работникам осуществляется при трудоустройстве, работниками управления по работе с персоналом. При выдаче на карту доступа наносятся фамилия, имя, отчество и фотография работника.

4.4. Выдача карт доступа обучающимся очной, очно-заочной и заочной формы обучения осуществляется в учебных частях соответствующих институтов и школ, аспирантам, лицам, прикрепленным для подготовки диссертации, лицам, прикрепленным для сдачи кандидатских экзаменов – в отделе аспирантуры и докторантуры, ученикам гимназии и обучающимся по программам дополнительного образования – в гимназии и соответствующих подразделениях университета.

4.5. Временные карты доступа выдаются работниками диспетчерской службы Центра информационных технологий (далее – ЦИТ). Для получения временной карты работник университета, ответственный за договор, в соответствии с которым необходимо предоставление доступа, направляет электронную служебную записку в системе электронного документооборота по утвержденному маршруту.

4.6. В случае утери или поломки *постоянной карты* доступа для получения новой карты:

- работники обращаются в управление по работе с персоналом;
- обучающиеся обращаются в диспетчерскую службу ЦИТ с заявлением об утере (поломке) карты доступа, заверенным специалистом по УМР своего института, школы, гимназии, работником отдела аспирантуры и докторантуры.

4.7. В случае утери или поломки *временной карты* доступа для получения новой карты работник, указанный в п. 4.5 настоящего положения, направляет электронную служебную записку в системе электронного документооборота по утвержденному маршруту.

4.8. Порядок выдачи карт доступа в филиалах университета при наличииСКУД определяет директор филиала.

4.9. Пульты для шлагбаумов и ворот предназначены только для проезда служебного автотранспорта, принадлежащего ТюмГУ, и выдаются водителям такого автотранспорта начальником отдела транспорта.

4.10. Пульты для шлагбаумов и ворот для проезда личных автомобилей работников не используются. Для проезда таких автомобилей используется метод GSM-идентификации.

5. Предоставление доступа

5.1. Здания и помещения университета с контролируемым доступом делятся на учебные, административные и служебные. Доступ в здания и помещения может предоставляться в зависимости от занимаемой должности или от исполняемых обязанностей.

5.2. При трудоустройстве работникам, при зачислении обучающимся очной формы обучения и лицам, прикрепленным для подготовки диссертации, лицам, прикрепленным для сдачи кандидатских экзаменов по умолчанию автоматически предоставляется доступ в учебные и административные помещения.

5.3. Доступ обучающимся заочной формы обучения, ученикам гимназии, обучающимся по программам дополнительного образования предоставляется по спискам, направляемым в виде электронной служебной записки в системе электронного документооборота по утвержденному маршруту.

5.4. Доступ в здания и помещения, необходимый в соответствии с должностными обязанностями, предоставляется работникам автоматически при приеме или переводе на данную должность и отзывается при увольнении или переводе на другую должность.

5.5. Для изменения уровня доступа в здания и помещения, необходимого в соответствии с функциональными обязанностями, работник,

которому требуется такой доступ, направляет электронную служебную записку в системе электронного документооборота по утвержденному маршруту.

5.6. Доступ в общежития предоставляется обучающимся и работникам, проживающим в этих общежитиях, по спискам, направляемым работником ответственного за расселение подразделения университета в виде электронной служебной записки в системе электронного документооборота по утвержденному маршруту.

5.7. Доступ в режимные помещения, оборудованные средствами СКУД, предоставляется на основании списков, утверждаемых приказом по университету.

5.8. Порядок предоставления доступа на территорию, в здания и помещения филиалов университета при наличии СКУД определяет директор филиала.

5.9. Доступ транспортных средств на территорию университета предоставляется:

- для служебного автотранспорта университета на основании списков, утвержденных приказом по университету;

- для личных автомобилей работников ТюмГУ на основании служебной записки, направляемой в системе электронного документооборота по утвержденному маршруту;

- для автомобилей посетителей на основании служебной записки, направляемой в системе электронного документооборота по утвержденному маршруту.

5.10. Временные рамки доступа назначаются в соответствии с Положением о пропускном и внутриобъектовом режиме, иными локальными нормативными актами Университета.

5.11. Предоставление доступа по запросам, оформленным в виде электронных служебных записок в соответствии с настоящим Положением,

осуществляется в течение 3 (трех) рабочих дней с момента получения электронной служебной записки исполнителем.

6. Порядок прохода

6.1. Проход в здания и помещения университета работниками, обучающимися и посетителями осуществляется с помощью карт доступа или иных идентификаторов, удовлетворяющих требованиям, указанным в Приложении.

6.2. Для прохода в здания и помещения университета необходимо приложить карту доступа или иной идентификатор к считывателю, расположенному на турникете или на стене рядом с дверью. В случае, если пользователю СКУД разрешен доступ в данное помещение или здание, считыватель издаст звуковой сигнал и отобразит световую индикацию зеленого цвета. В случае, если пользователю СКУД доступ не разрешен, считыватель издаст звуковой сигнал и отобразит световую индикацию красного цвета.

6.3. Открытие турникетов с кнопки работником охраны может производиться только для прохода лиц, не являющихся пользователями СКУД, в сопровождении ответственного работника университета после занесения в журнал охраны фамилии, имени, отчества и данных документа посетителя. Таким документом может быть:

- удостоверение личности;
- удостоверение работника скорой медицинской помощи, прибывшего по вызову в здание университета;
- служебное удостоверение сотрудника правоохранительных органов, прибывшего по вызову в соответствии с законодательством Российской Федерации для исполнения служебных обязанностей;
- служебное удостоверение сотрудника контрольных или надзорных органов, прибывшего в университет с целью проведения проверки, предусмотренной законодательством Российской Федерации и приказом (распоряжением) о проведении проверки.

6.4. Открытие турникета с кнопки работником охраны для прохода пользователей СКУД, карта или иной идентификатор которых утерян или сломан, осуществляется после предъявления удостоверения работника или удостоверения аспиранта университета, студенческого билета обучающегося университета и занесения в журнал охраны данных предъявленного документа.

6.5. Открытие турникета с кнопки работником охраны для прохода участников мероприятий, проходящих в зданиях университета, осуществляется после предъявления участником мероприятия удостоверения личности при наличии данного участника в списках, предоставляемым ответственным за мероприятие в виде электронной служебной записки в системе электронного документооборота по утвержденному маршруту.

6.6. В случае выхода из строя оборудования СКУД вход осуществляется при предъявлении следующих документов:

- для работников – удостоверения работника ТюмГУ или персонифицированной карты доступа;
- для обучающихся – студенческого билета, зачетной книжки, удостоверения аспиранта, персонифицированной карты доступа;
- для посетителей – удостоверения личности с занесением в журнал охраны данных предъявленного документа.

6.7. Проход в праздничные и выходные дни осуществляется в соответствии с Положением о пропускном и внутриобъектовом режиме, иными локальными нормативными актами университета.

6.8. Турникеты в обычном состоянии должны быть заблокированы как на вход, так и на выход. В случае возникновения чрезвычайной ситуации работник охраны разблокирует турникеты и калитки «антипаника».

6.9. Въезд транспорта на территорию университета осуществляется через контрольно-пропускные пункты, оборудованные автоматическими шлагбаумами или воротами. Открытие шлагбаума или ворот происходит по нажатию кнопки на пульте от данного шлагбаума или по звонку

на выделенный номер телефона, если шлагбаум оборудован GSM-модулем. Открытие шлагбаума или ворот для проезда транспорта обслуживающих организаций (доставка товара, инкассация и т.п.) осуществляется работником охраны с кнопки или пульта.

7. Права и обязанности пользователей СКУД

7.1. Пользователь СКУД имеет право:

- проходить в здания и помещения университета в соответствии с назначенным уровнем доступа;
- получить новую карту доступа в случае утери или поломки старой;
- использовать для прохода в здания и помещения университета идентификаторы, удовлетворяющие требованиям, приведенным в Приложении (только для пользователей СКУД, являющихся работниками университета);
- по вопросам, связанным с проходом в здания и помещения, работой СКУД обращаться к работникам охраны или в диспетчерскую службу ЦИТ.

7.2. Пользователь СКУД обязан:

- предъявлять карту доступа или иной идентификатор по требованию работника охраны;
- для прохода в здания и помещения университета использовать только свою карту доступа или иной личный идентификатор;
- бережно относиться к средствам контроля и управления доступом;
- в случае утери или повреждения карты доступа или иного идентификатора незамедлительно сообщить в диспетчерскую службу ЦИТ;
- соблюдать требования настоящего Положения;
- сообщать о нарушении требований настоящего положения сотрудникам охраны;
- сообщать об обнаруженных неисправностях или сбоях в работе СКУД сотрудникам охраны.

7.3. Пользователю СКУД запрещается:

- передавать свою карту доступа или иной идентификатор другим лицам;
- пропускать в здания и помещения университета по своей карте или иному идентификатору других лиц;
- пользоваться картой доступа или иным идентификатором другого лица;
- пролезать под турникетом, перепрыгивать турникет или обходить его иным способом;
- самостоятельно копировать информацию с карты доступа на другие носители;
- вносить изменения в конструкцию карты доступа или любым способом модифицировать ее.

8. Ответственность

8.1. Ответственность за организацию работы СКУД возлагается на ЦИТ.

8.2. Ответственность за поддержание работоспособности подсистем СКУД регламентируется локальными нормативными документами университета.

8.3. Ответственность за обеспечение пропускного режима с использованием средств СКУД возлагается на службу главного инженера и охранную организацию, предоставляющую ТюмГУ услуги по охране территории и объектов университета на основании контракта.

8.4. Пользователи СКУД несут ответственность за выполнение требований настоящего Положения. Нарушение требования настоящего Положения влечет за собой дисциплинарную ответственность, а также уголовную или административную, если это предусмотрено законодательством Российской Федерации.

Приложение к Положению
о системе контроля и управления
доступом в федеральном
государственном автономном
образовательном учреждении
высшего образования
«Тюменский государственный
университет»

Характеристики карт доступа и идентификаторов

Идентификаторы, используемые в системе контроля и управления доступом в университете должны обладать следующими характеристиками:

- рабочая частота: 13,56 МГц и 125 кГц;
- используемый стандарт: EM-Marine, HID ProxCard II, Mifare, NFC, ISO14443-A;
- бесконтактные банковские карты: MasterCard, Visa, МИР;
- смартфоны с операционными системами Android (версии не ниже 7.0), iOS (версии не ниже 9), поддерживающие технологию BLE.