	Частное образовательное учреждение высшего образования **«ЗАПАДНО-УРАЛЬСКИЙ ИНСТИТУТ ЭКОНОМИКИ И ПРАВА»** **(ЧОУ ВО «ЗУИЭП»)** г. Пермь	
	Система менеджмента качества	
	Положение	
СМК-П- 03.36-19	**О корпоративной компьютерной сети Частного образовательного учреждения высшего образования «Западно-Уральский институт экономики и права»**	**Версия 01**

УТВЕРЖДАЮ
Ректор института
_____ Н.Н. Агафонова
19 апреля 2019 г.

ПОЛОЖЕНИЕ О КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ ЧАСТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЗАПАДНО-УРАЛЬСКИЙ ИНСТИТУТ ЭКОНОМИКИ И ПРАВА»

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение определяет основные принципы и правила функционирования корпоративной компьютерной сети Частного образовательного учреждения высшего образования «Западно-Уральский институт экономики и права» (далее - Институт, ЧОУ ВО «ЗУИЭП»), а также права, обязанности и ответственность участников корпоративной компьютерной сети.

1.2. Настоящее Положение предназначено для создания нормативной основы регулирования информационных процессов в корпоративной компьютерной сети, организации совместной работы в корпоративной компьютерной сети структурных подразделений Института и отдельных пользователей.

1.3. Соблюдение требований настоящего Положения отвечает интересам Института и является обязательным для всех участников корпоративной компьютерной сети.

1.4. Настоящее Положение является внутренним документом и распространяется на работников и обучающихся Института.

1.5. Положение входит в состав документации, обеспечивающей функционирование системы менеджмента качества.

2. НОРМАТИВНЫЕ ПРАВОВЫЕ ОСНОВАНИЯ

- ГОСТ Р 54623-2011 Информационно-коммуникационные технологии в образовании. Системы зданий образовательного назначения технологические информационно-коммуникационные. Термины и определения.
- ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
- Устав ЧОУ ВО «ЗУИЭП»;

- Локальные акты, регулирующие образовательную деятельность ЧОУ ВО «ЗУИЭП».

3. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3.1. Термины, определения

Данные - информация, представленная на электронном носителе в цифровой форме, пригодной для обработки программами вычислительной техники.

Идентификационные данные - это данные, которые уникальным образом характеризуют работника, обучающегося или объект.

Информационная система - совокупность содержащейся в базах данных информации и информационных технологий и технических средств, обеспечивающих ее обработку.

Информационная технология - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления этих процессов и методов.

Информационно-коммуникационная технологическая система - совокупность инженерного оборудования и информационных технологий, предназначенных для комплексного управления технологическими процессами с применением средств вычислительной техники и телекоммуникаций.

Информационно-коммуникационная технология - информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации.

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы - переведенная в цифровой код информация в форме данных, баз данных и программно-информационных продуктов, которая обрабатывается с использованием средств вычислительной техники.

Информационный процесс - процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

Кабельная система - совокупность физических каналов, предназначенных для передачи электрических и оптических сигналов, включающих телекоммуникационные кабели и элементы коммутации.

Локальная сеть - объединение терминального, сетевого и периферийного оборудования помещения или комплекса помещений с помощью кабельной системы и радиоканалов с целью совместного использования аппаратных и сетевых ресурсов и периферийного оборудования.

Несанкционированный доступ - доступ к информации или к ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа.

Рабочее место - часть помещения, оснащенная терминальным оборудованием и интерфейсом структурированной кабельной системы и предназначенная для работы одного пользователя.

Структурированная кабельная система — кабельная система здания, предназначенная для передачи телекоммуникационных сигналов, построенная по

общепринятым стандартам, составляющая телекоммуникационную инфраструктуру указанного здания.

Телекоммуникационная розетка - окончание кабеля, оснащенное гнездовым разъемом и предназначенное для подключения терминального или периферийного оборудования.

Терминальное оборудование - оборудование, подключенное к информационно-телекоммуникационной сети, являющееся источником и потребителем информации, преобразующее информацию в данные и осуществляющее обратное преобразование.

Узел связи - совокупность аппаратных и программных средств, обеспечивающих маршрутизацию трафика и присоединение корпоративной компьютерной сети к сетям общего пользования.

3.2. Принятые сокращения

ИС- информационные системы;

ИТ - информационная технология;

ИТС- информационно-телекоммуникационная сеть;

ИКС - корпоративная компьютерная сеть;

ЛКС-локальная компьютерная сеть;

УМУ - учебно-методическое управление;

Институт, ЧОУ ВО «ЗУИЭП» - Частное образовательное учреждение высшего образования «Западно-Уральский институт экономики и права».

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Корпоративная компьютерная сеть является технологической основой функционирования ИТ-среды Института, обеспечивающей информационную поддержку учебной, научной и административной деятельности.

4.2. ККС Института выполняет функции объединения структурных подразделений Института в единую информационно-коммуникационную технологическую систему, способствует формированию единого научно-образовательного пространства Института и его интеграцию в мировое информационное пространство.

4.3. ККС представляет собой организационно-технологический комплекс, на основе технологий Ethernet и стека протоколов TCP/IP, объединяющий локальные компьютерные сети, отдельные рабочие места, серверы, прочее терминальное оборудование, связанные между собой проводным способом с использованием сетевого оборудования, в единую сеть. Указанные составляющие ККС могут располагаться как на территории Института, так и на площадях, арендуемых у сторонних организаций.

5. ОСНОВНЫЕ ЗАДАЧИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

5.1. ККС Института предназначена для решения следующих основных задач:

- обеспечение информационного взаимодействия структурных подразделений Института, отдельных работников и обучающихся;
- обеспечение надежного и эффективного доступа к глобальной сети Интернет;
- обеспечение эффективного сбора, обработки, хранения, распространения, поиска, передачи и защиты информации;
- создание условий развития и внедрения новых информационно-коммуникационных

технологий в основные направления деятельности Института;
- интеграция различных информационных ресурсов и систем Института на основе современных информационно-коммуникационных технологий.

6. СТРУКТУРА КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

6.1. Основными компонентами ККС являются:
- узлы связи Института;
- базовая информационно-телекоммуникационная сеть Института;
- локальные компьютерные сети подразделений;
- информационные системы.

6.2. Узлы связи Института обеспечивают интеграцию компонентов ККС, а также маршрутизацию трафика в глобальную сеть Интернет. В состав узлов входит активное сетевое и серверное оборудование, в том числе коммутаторы, маршрутизаторы, межсетевые экраны.

6.3. Базовая ИТС Института обеспечивает коммутацию и передачу данных между отдельными компонентами ККС. В ее состав входят кабельные линии связи, коммутационное оборудование, в том числе коммутаторы уровня агрегации и уровня доступа, а также каналы связи, арендуемые у операторов связи на основании договоров или организованные через общие сети связи, точки подключения рабочих мест и компонентов ККС в виде телекоммуникационных розеток.

6.4. ЛКС подразделений функционируют в интересах отдельных структурных подразделений Института и объединяют компьютеры и другое терминальное оборудование, в том числе в составе компьютерных классов, закрепленные за подразделениями Института. Локальные сети могут быть как проводными, так и беспроводными, создаются и обслуживаются подразделениями в соответствии с настоящим Положением и другими локальными нормативными актами Института.

6.5. Беспроводные сети в Институте организуются в соответствии с Приложением 1 настоящего Положения.

6.6. Информационные системы размещаются на серверах Института и/или структурных подразделений и могут быть:
- публично доступные - системы и сервисы, доступные пользователям внешних сетей, такие как web-сайты, электронная почта и т.д.;
- корпоративные — системы и сервисы, доступные для различных групп пользователей Института, такие как внутренний информационный портал, внутренняя электронная почта, система документооборота и т.д.;
- ресурсы подразделений — системы и сервисы, доступные работникам отдельных подразделений, такие как файловые серверы, сервисы совместной разработки и т.д.

7. ПОРЯДОК ПОДКЛЮЧЕНИЯ К КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

7.1. Подключение рабочих мест, локальных компьютерных сетей подразделений, серверов информационных систем к ККС заключается в монтаже кабельной системы и телекоммуникационной розетки, подключенной к базовой ИТС, осуществляется

проводным способом.

8. БЕЗОПАСНОСТЬ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

8.1. Обеспечение информационной безопасности предусматривает комплекс организационных, технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний, злоупотреблений в отношении компонентов ККС.

8.2. К организационным мероприятиям относятся:

- ознакомление участников ККС с настоящим Положением и контроль соблюдения требований настоящего Положения;
- разработка локальных нормативных актов в области регулирования ИТ-среды Института и их исполнение;
- ограничение доступа работников, обучающихся и посетителей в помещения, в которых расположены серверы и телекоммуникационное оборудование;

8.3. К техническим мероприятиям относятся:

- логическое и физическое сегментирование ККС Института с разграничением доступа между сегментами;
- применение межсетевых экранов и контентных фильтров;
- ограничение функционирования отдельных сетевых протоколов,
- применение парольной и установка на компьютерном оборудовании специализированного антивирусного программного обеспечения;
- приобретение и использование сертифицированного оборудования, гарантирующего надежную работу самого оборудования и информационных систем;
- размещение серверов ККС в специально оборудованном помещении, исключающем несанкционированный доступ и обеспечивающем требуемый режим работы оборудования;
- приобретение и использование лицензионного программного обеспечения, своевременное обновление программного обеспечения;
- регулярное резервное копирование критичной для функционирования информации;
- мониторинг действий пользователей в ККС Института.

9. ТРЕБОВАНИЯ К РАБОТЕ В ККС

9.1. При работе в ККС запрещается;

- самовольное подключение к ККС;
- организация точек доступа к ККС для третьих лиц, а также организация удаленного доступа без согласования с руководством ККС;
- установка точек беспроводного доступа без согласования с руководством ККС;
- физическое повреждение компонентов ККС;
- разглашение идентификационных данных;
- незаконное распространение персональных данных сотрудников и обучающихся;
- сканирование сети и подбор паролей других пользователей;
- использование чужих сетевых атрибутов (в частности, IP-адресов, MAC- адресов) и/или идентификационных данных;
- подмена адреса отправителя при использовании электронной почты;
- массовая несанкционированная руководством рассылка электронных сообщений

(спам);

- разработка или распространение вредоносного программного обеспечения;
- проведение сетевых атак;
- несанкционированный доступ или попытки несанкционированного доступа к информации;
- необоснованная производственной необходимостью загрузка сети;
- распространение информации, запрещенной законодательством РФ;
- распространение информации, противоречащей нормам морали и нравственности, порочащей честь и достоинство граждан, рассылка обманных или угрожающих сообщений;
- нарушение авторских прав, модификация, повреждение, удаление не принадлежащих пользователю данных;
- использование ККС в деятельности, противоречащей законодательству РФ.

При выявлении нарушений необходимо принять меры по их пресечению, проинформировать руководство ККС о нарушении и принятых мерах.

9.2. Нарушители частично или полностью отстраняются от пользования ККС и несут ответственность в соответствии с законодательством РФ и локальными нормативными актами Института.

9.3. Общая политика заключается в том, что при обнаружении нарушений, проблем или сбоев в сети, а также больших потоков трафика, производится временное отключение пользователя или компонента ККС до выяснения и устранения причин.

9.4. При возникновении в структурном подразделении Института проблем в работе с ККС, требующих выяснения внутренних причин, поиска внутренних нарушителей или проведения внутренних расследований, эти действия осуществляются работниками этого подразделения.

10. Заключительные положения

10.1. Настоящее Положение подписывается разработчиком, согласовывается с начальником учебно-методического управления, юрисконсультом и утверждается ректором Института.

10.2. Контрольный экземпляр Положения регистрируется и хранится на бумажном носителе и в электронной базе документов СМК. В канцелярию Института на хранение передается учтенный экземпляр Положения на бумажном носителе.

10.3. Учтенный экземпляр (копию контрольного экземпляра) Положения согласно реестру внутренней рассылки документов канцелярия передает в заинтересованные структурные подразделения.

10.4. Изменения и дополнения в Положение вносятся по предложению заинтересованных лиц. Предложения представляются проректору по образовательной деятельности в письменном виде для согласования. Изменения и дополнения в настоящее Положение утверждаются ректором Института и фиксируются в листе регистрации изменений.

10.5. Новая версия Положения с внесенными изменениями доводится до сведения сотрудников структурных подразделений под подпись.

РАЗРАБОТАНО:

Системный администратор _____ А.В. Чаднов

(личная подпись) (расшифровка подписи)

17 апреля 2019 г.

СОГЛАСОВАНО:

Начальник учебно-методического управления	(личная подпись)	И.И. Лобанова (расшифровка подписи)
17 апреля 2019 г.		
Юрисконсульт	(личная подпись)	Т.А. Сидорук (расшифровка подписи)
17 апреля 2019 г.		
Председатель студенческого совета	(личная подпись)	К.А. Шишкина (расшифровка подписи)
17 апреля 2019 г.		

ВВЕДЕНО В ДЕЙСТВИЕ приказом от «19» апреля 2019 г. № 12-ОД

Приложение 1

Организация работы беспроводных сетей в ЧОУ ВО «ЗУИЭП»

1. Беспроводные сети в Институте представлены беспроводными сетями структурных подразделений и публичными беспроводными сетями.
2. Беспроводные сети структурных подразделений являются локальными компьютерными сетями подразделений.
3. Беспроводные сети подразделений не являются публичными и должны быть защищены паролем и доступны лишь зарегистрированным пользователям.
4. Рекомендации к организации беспроводных сетей:

- имя сети (SSID) состоит из сокращенного названия подразделения и номера аудитории, в которой размещена точка доступа;
- длина пароля составляет не менее 8 символов;
- в числе символов пароля обязательно присутствуют буквы латинского алфавита в верхнем и нижнем регистре и цифры или специальные символы;
- пароль не должен записываться или передаваться открытым текстом в электронных сообщениях;
- смена пароля производится не реже одного раза в 3 месяца;
- новый пароль должен отличаться от предыдущего не менее чем в 5 позициях;
- пароль для доступа к беспроводной сети должен отличаться от пароля для настройки точки доступа;
- протокол безопасности WPA2;
- применяется фильтр MAC-адресов для разрешения доступа с ограниченного количества устройств;
- служба WPS отключена.

5. В случае компрометации либо подозрения на компрометацию пароля необходимо сообщить об этом администратору беспроводной сети. Администратор в свою очередь должен немедленно изменить пароль.
6. При организации беспроводной сети структурного подразделения точки беспроводного доступа должны быть зарегистрированы в УИ.
7. Публичные беспроводные сети в Институте организуются оператором связи на основании договора и в соответствии с законодательством РФ. Публичные беспроводные сети не интегрируются в ККС и используются для доступа к сети Интернет.

Лист регистрации изменений

Номер изменения	Номер и дата распорядительного документа о внесении изменений в документ СМК	Номер страницы	Описание изменения		ФИО и подпись лица, внесшего изменение
			Старая версия	Новая версия	