

Документ подписан с помощью электронной подписью

Информация о владельце

ФИО: Лизунова Лариса Рейнрида

Должность: Проректор по образовательной деятельности и информатизации

Дата подписания: 25.05.2022 12:37:58

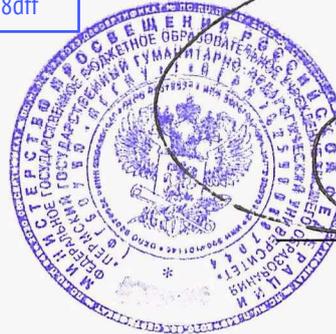
Уникальный программный ключ:

2df9c6861881908afc45bec7d3c3932fa758d4b545fa3be46a642db74e588dff

Система менеджмента качества СТО ПП-02-02-2022

ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»

Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ



«Утверждаю»

Ректор ПГГПУ

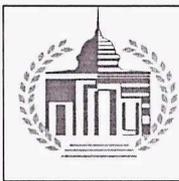
К.Б. Егоров

« 11 » мая 2022 г.

ПОЛОЖЕНИЕ

О КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ ФГБОУ ВО ПГГПУ

Пермь
2022



Система менеджмента качества СТО ПП-02-02-02-2022

ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»

Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

Предисловие

1. Разработано:
Лизунова Л.Р., проректор по образовательной деятельности и информатизации,
Гавриков О.В., начальник управления информатизации ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет».
2. Утверждено Ученым советом ПГГПУ, протокол № 7 от 26.04.2022 г.
3. Введено в действие распоряжением ректора ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет» № 53 от 11 мая 2022 г.
4. Введено взамен: СТО ПП-02-02-01-2019 «Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ».

Периодичность ПЕРЕСМОТРА стандарта организации 1 раз в 3 года.

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без письменного разрешения ректора ПГГПУ.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

СОДЕРЖАНИЕ

1.	Назначение и область применения	4
2.	Нормативно-правовые основания	4
3.	Обозначения и сокращения	4
4.	Общие положения	6
5.	Основные задачи корпоративной компьютерной сети	7
6.	Структура корпоративной компьютерной сети	7
7.	Участники корпоративной компьютерной сети	8
8.	Права, обязанности, ответственность и полномочия участников ККС	9
9.	Порядок подключения к корпоративной компьютерной сети	14
10.	Безопасность в корпоративной компьютерной сети	15
11.	Требования к работе в ККС	16
12.	Согласование, хранение и рассылка	17
13.	Порядок внесения изменений	17
	<i>Приложение А. Организация работы беспроводных сетей в ФГБОУ ВО ПГГПУ</i>	18
	<i>Приложение Б. Лист регистрации изменений</i>	19
	<i>Приложение В. Лист согласования</i>	20



1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение определяет основные принципы и правила функционирования корпоративной компьютерной сети федерального государственного бюджетного образовательного учреждения высшего образования «Пермский государственный гуманитарно-педагогический университет» (далее – Университет, ПГГПУ), 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 Университета и отдельных пользователей.

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

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

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

2. НОРМАТИВНО-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 федерального государственного бюджетного образовательного учреждения высшего образования «Пермский государственный гуманитарно-педагогический университет»;
- Локальные акты, регулирующие образовательную деятельность ФГБОУ ВО ПГГПУ.

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.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

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

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

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

ИТ – информационная технология;

ИТС – информационно-телекоммуникационная сеть;

ККС – корпоративная компьютерная сеть;

ЛКС – локальная компьютерная сеть;

ОМККО - отдел мониторинга и контроля качества образования Университета;

УИ – управление информатизации Университета;

УМУ – учебно-методическое управление Университета;

Университет, ПГГПУ - федеральное государственное бюджетное образовательное учреждение высшего образования «Пермский государственный гуманитарно-педагогический университет».

4. ОБЩИЕ ПОЛОЖЕНИЯ

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

4.2. ККС Университета выполняет функции объединения структурных подразделений Университета в единую информационно-коммуникационную технологическую систему, способствует формированию единого научно-образовательного пространства Университета 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 Университета, так и на площадях, арендуемых у сторонних организаций.

4.4. Доступ в ККС работникам, обучающимся Университета предоставляется сотрудниками Управления информатизации на основании приказов ректора о зачислении или движении контингента сотрудников.

4.5. Управление ККС и ее развитие осуществляется под руководством управления информатизации в лице начальника и работников управления информатизации в соответствии с их должностными инструкциями.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

5. ОСНОВНЫЕ ЗАДАЧИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

5.1. ККС Университета предназначена для решения следующих основных задач:

- обеспечение информационного взаимодействия структурных подразделений Университета, 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 Университета;
- интеграция различных информационных ресурсов и систем Университета на основе современных информационно-коммуникационных технологий.

6. СТРУКТУРА КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

6.1. Основными компонентами ККС являются:

- узлы связи Университета;
- базовая информационно-телекоммуникационная сеть Университета;
- локальные компьютерные сети подразделений;
- информационные системы.

6.2. Узлы связи Университета 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 Университета 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 Университета и объединяют компьютеры и другое терминальное оборудование, в том числе в составе компьютерных классов, закрепленные за подразделением. Локальные сети могут быть как проводными, так и беспроводными, создаются и обслуживаются подразделениями в соответствии с настоящим Положением и другими локальными нормативными актами Университета.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГПУ

6.5. Беспроводные сети в ПГПУ организуются в соответствии с Приложением А настоящего Положения.

6.6. Информационные системы размещаются на серверах Университета 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 Университета, 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. УЧАСТНИКИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

7.1. Участниками ККС являются:

- ответственное руководство ККС;
- администраторы ККС Университета;
- администраторы ЛКС подразделений;
- администраторы ИС;
- пользователи ККС Университета.

7.2. Ответственное руководство ККС в составе начальника УИ, начальников отделов УИ определяет стратегию развития ККС, требования к ее компонентам с целью обеспечения высокого уровня информатизации Университета.

7.3. Администраторы ККС Университета – работники УИ, осуществляющие контроль, поддержание работы, обеспечение безопасности, развитие и модернизацию узлов связи и базовой информационно-телекоммуникационной сети Университета.

7.4. Администраторы локальных компьютерных сетей подразделений осуществляют создание, контроль, обслуживание, обеспечение безопасности ЛКС. Администраторами ЛКС подразделения являются работники этого подразделения, обладающие необходимыми знаниями и навыками и назначаемые распоряжением руководителя структурного подразделения. В случае не назначения администратора ответственность за функционирование ЛКС возлагается на руководителя подразделения.

7.5. Администраторы информационных систем осуществляют контроль, обслуживание, обеспечение безопасности ИС. Администраторами ИС являются работники подразделения, разработавшего или внедрившего соответствующую систему, обладающие необходимыми навыками и назначаемые распоряжением руководителя структурного подразделения. В случае не назначения администратора ответственность за функционирование ИС возлагается на руководителя подразделения.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

7.6. Пользователи ККС – работники, обучающиеся и иные лица, использующие услуги, предоставляемые компонентами ККС Университета.

8. ПРАВА, ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ УЧАСТНИКОВ ККС

8.1. Права, обязанности и ответственность руководства ККС Университета:

8.1.1. Обязанности руководства ККС:

- знать и выполнять требования законодательства РФ, настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;
- определять стратегию и осуществлять планирование развития ККС и отдельных ее компонентов;
- осуществлять организацию работы в ККС в соответствии с законодательством РФ и локальными нормативными актами Университета;
- взаимодействовать с руководством Университета и внешними организациями в вопросах работы и развития ККС Университета;
- доводить до сведения заинтересованных участников ККС информацию о решениях руководства ККС и руководства Университета, об изменениях в работе ККС;
- осуществлять руководство деятельностью администраторов ККС и ИС Университета;
- оказывать информационную и материально-техническую помощь администраторам ККС в исполнении их обязанностей.

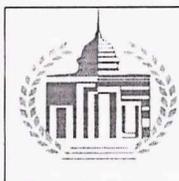
8.1.2. Права руководства ККС:

- осуществлять контроль деятельности администраторов ККС и ИС Университета;
- запрашивать отчеты по работе ККС и отдельных ее компонентов;
- разрабатывать локальные акты, обязательные к исполнению участниками ККС, направленные на развитие и улучшение функциональности ККС Университета;
- требовать от участников ККС исполнения требований настоящего положения;
- получать и принимать предложения по развитию и улучшению функциональности ККС или отдельных ее компонентов.

8.1.3. Ответственность руководства ККС.

Руководство ККС несет ответственность за:

- функционирование ККС в целом;
- обеспечение информационной безопасности ККС;
- соответствие ККС требованиям законодательства и локальных нормативных актов Университета;
- соответствие ККС современному уровню развития ИТ.



8.2. Права, обязанности и ответственность администраторов ККС:

8.2.1. Администратор ККС обязан:

- знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;
- обеспечивать установку, настройку и обновления программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети Университета;
- обеспечивать информационную безопасность программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети Университета;
- обеспечивать резервное копирование критичной для функционирования узлов связи и базовой информационно-телекоммуникационной сети информации;
- ограничивать доступ работников и посетителей в помещения узлов связи Университета;
- проводить работы, связанные с внедрением новых технологий и развитием узлов связи и базовой информационно-телекоммуникационной сети Университета;
- проводить периодический контроль работы узлов связи и базовой информационно-телекоммуникационной сети Университета;
- в случае отказа работоспособности программных и аппаратных элементов узлов связи и базовой информационно-телекоммуникационной сети Университета принимать меры по их восстановлению и выявлению причин, приведших к отказу;
- информировать руководство ККС об отказах работоспособности и нарушениях или попытках нарушений информационной безопасности узлов связи и базовой информационно-телекоммуникационной сети Университета;
- оповещать участников ККС об изменениях в работе узлов связи и базовой информационно-телекоммуникационной сети, влияющих на их работу.

8.2.2. Администратор ККС имеет право:

- давать участникам ККС обязательные к исполнению указания и рекомендации по вопросам работы и соблюдения информационной безопасности в ККС;
- осуществлять контроль информационных потоков в ККС;
- отключать от ККС ЛКС, ИС, отдельные рабочие места и пользователей, нарушающих ее работу, а также в случаях злоупотребления сетью, нарушений требований настоящего Положения и других локальных нормативных актов Университета;
- запрашивать и получать от руководителей и специалистов структурных подразделений Университета информацию и материалы, необходимые для организации своей работы;

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

- запрашивать и получать от руководства ККС информационное и материально-техническое обеспечение деятельности, а также оказание содействия в исполнении своих обязанностей;

- вносить на рассмотрение руководства ККС предложения по развитию и улучшению функциональности ККС.

8.2.3. Ответственность администратора ККС.

Администратор ККС несет ответственность за:

- функционирование узлов связи и базовой информационно-телекоммуникационной сети;

- обеспечение информационной безопасности элементов узлов связи и базовой информационно-телекоммуникационной сети;

- выполнение требований настоящего положения.

Администратор ККС не несет ответственность за:

- содержание проходящих по сети данных;

- информацию, находящуюся в ИС, в ЛКС подразделений, на компьютерах пользователей и другом терминальном оборудовании;

- работоспособность ИС, ЛКС подразделений, компьютеров пользователей и другого терминального оборудования;

- работоспособность и физическое состояние линий связи в ЛКС подразделений.

8.3. Права, обязанности и ответственность администраторов ЛКС

Университета.

8.3.1 Администратор ЛКС обязан:

- знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;

- организовывать работу ЛКС таким образом, чтобы она не нарушала работоспособности других компонентов ККС;

- обеспечивать информационную безопасность программных и аппаратных элементов ЛКС;

- обеспечивать резервное копирование критичной для функционирования ЛКС информации;

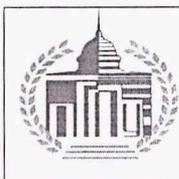
- ограничивать доступ работников и посетителей к программным и аппаратным элементам ЛКС;

- проводить контроль работы ЛКС;

- в случае нарушения работоспособности ЛКС принимать меры по ее восстановлению и выявлению причин, приведших к нарушению;

- информировать непосредственного руководителя об отказах работоспособности и нарушениях или попытках нарушений информационной безопасности ЛКС;

- оповещать администраторов ККС и других участников ККС об изменениях в работе ЛКС, влияющих на их работу;



– содействовать администраторам ККС и руководству ККС в организации работы ККС.

8.3.2. Администратор ЛКС имеет право:

– давать пользователям ЛКС обязательные к исполнению указания и рекомендации по вопросам работы и соблюдения информационной безопасности в ЛКС;

– осуществлять контроль информационных потоков в ЛКС;

– отключать от ЛКС, ИС, отдельные рабочие места и пользователей, нарушающих ее работу, а также в случае злоупотребления сетью, нарушений требований настоящего положения и других локальных нормативных актов Университета;

– развивать и модернизировать ЛКС в соответствии с общим развитием ИТ-среды Университета;

– запрашивать и получать от администраторов ККС консультативную помощь в вопросах организации правильной работы ЛКС в ККС Университета;

– вносить на рассмотрение администраторов ККС предложения по развитию и улучшению функциональности ККС.

8.3.3. Ответственность администраторов ЛКС. Администратор ЛКС несет ответственность:

– за функционирование ЛКС подразделения;

– за обеспечение информационной безопасности элементов ЛКС;

– в случае нарушения работоспособности компонентов ККС в результате некорректного управления ЛКС подразделения;

– за выполнение требований настоящего Положения.

8.4. Права, обязанности и ответственность администраторов ИС Университета.

8.4.1 Администратор ИС обязан:

– знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;

– организовывать работу ИС таким образом, чтобы она не нарушала работоспособности других компонентов ККС;

– осуществлять контроль устанавливаемого и/или разрабатываемого программного обеспечения ИС на предмет соответствия законодательству РФ, в том числе на предмет соблюдения авторских прав;

– обеспечивать информационную безопасность программных и аппаратных элементов ИС;

– обеспечивать резервное копирование критичной для функционирования ИС информации;

– ограничивать доступ работников и посетителей к программным и аппаратным элементам ИС;

– проводить контроль работы ИС;

	Система менеджмента качества СТО ПП-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

- в случае нарушения работоспособности ИС принимать меры по ее восстановлению и выявлению причин, приведших к нарушению;

- информировать непосредственного руководителя об отказах работоспособности и нарушениях или попытках нарушений информационной безопасности ИС

- оповещать участников ККС об изменениях в работе ИС, влияющих на их работу;

- содействовать администраторам и руководству ККС в организации работы ККС.

8.4.2. Администратор ИС имеет право:

- давать пользователям ИС обязательные к исполнению указания и рекомендации по вопросам работы и соблюдения информационной безопасности в ИС;

- осуществлять контроль информационных потоков в ИС;

- отключать от ИС пользователей, нарушающих ее работу, а также в случае нарушений требований настоящего положения и других локальных нормативных актов Университета;

- развивать и модернизировать ИС в соответствии с общим развитием ИТ-среды Университета;

- запрашивать и получать от администраторов ККС консультативную помощь в вопросах организации правильной работы ИС в ККС Университета;

- вносить на рассмотрение руководства и администраторов ККС предложения по развитию и улучшению функциональности ККС.

8.4.3 Ответственность администраторов ИС.

Администратор ИС несет ответственность:

- за функционирование ИС;

- за обеспечение информационной безопасности ИС;

- в случае нарушения работоспособности компонентов ККС в результате некорректной настройки и управления ИС;

- за выполнение требований настоящего положения.

8.5. Права, обязанности и ответственность пользователей ККС.

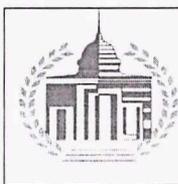
8.5.1. Пользователь обязан:

- знать и выполнять требования настоящего положения и других локальных нормативных актов в области регулирования ИТ-среды Университета;

- использовать ККС только в профессиональных, служебных и учебных целях;

- обеспечивать информационную безопасность рабочего места, в том числе парольную и антивирусную защиту;

- хранить в тайне свои идентификационные данные;



- препятствовать несанкционированному и недобросовестному использованию ККС;
- об изменении конфигурации рабочего места сообщать администратору ККС или ЛКС, к которой рабочее место подключено;
- не устанавливать на рабочем месте сетевые сервисы без согласования с администратором ККС или ЛКС, к которой рабочее место подключено.

8.5.2. Пользователь имеет право:

- получать доступ к информационным ресурсам ККС в профессиональных и служебных целях;
- получать доступ во внешние сети, в том числе в глобальную сеть Интернет в профессиональных и служебных целях;
- запрашивать и получать от администраторов ККС и/или ЛКС консультативную помощь в вопросах правильной организации работы в ККС Университета.

8.5.3. Ответственность пользователей ККС.

Пользователь ККС несет ответственность:

- за любые действия, совершенные с использованием его идентификационных данных или с закрепленного за ним рабочего места;
- за соблюдение информационной безопасности рабочего места, в том числе парольной и антивирусной защиты;
- в случае нарушения работоспособности компонентов ККС в результате некорректной настройки рабочего места или действий пользователя;
- за выполнение требований настоящего Положения.

9. ПОРЯДОК ПОДКЛЮЧЕНИЯ К КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

9.1. 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 и производится работниками отдела технической поддержки и системного администрирования управления информатизации совместно с сотрудниками эксплуатационно-технического отдела административно-хозяйственного управления.

9.2. Подключение к ККС осуществляется на основании служебной записки руководителя подразделения, согласованной с начальником управления информатизации и начальником административно-хозяйственного управления.

9.3. При подключении ИС к ККС данная ИС подлежит регистрации в УИ. При регистрации определяются функции, назначение и состав ИС, размещение ИС, администратор ИС, сетевые настройки для работы в ККС, доступность из других сетей, необходимость и ограничения использования сети Интернет, другие необходимые для подключения параметры, подтверждаемые руководителем подразделения.



10. БЕЗОПАСНОСТЬ В КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

10.1. Политика обеспечения информационной безопасности в ККС Университета строится руководством ККС совместно с администраторами ККС и администраторами ИС в соответствии с законодательством РФ и локальными нормативными актами Университета.

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

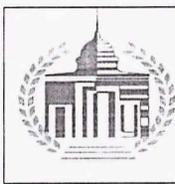
10.3. К организационным мероприятиям относятся:

- ознакомление участников ККС с настоящим Положением и контроль соблюдения требований настоящего Положения;
- разработка локальных нормативных актов в области регулирования ИТ-среды Университета и их исполнение;
- организация взаимодействия администраторов ККС, администраторов ЛКС и администраторов ИС;
- ограничение доступа работников, обучающихся и посетителей в помещения, в которых расположены серверы и телекоммуникационное оборудование;
- регистрация пользователей ЛКС и ИС с назначением прав доступа.

10.4. К техническим мероприятиям относятся:

- логическое и физическое сегментирование ККС Университета с разграничением доступа между сегментами;
- применение межсетевых экранов и контентных фильтров;
- ограничение функционирования отдельных сетевых протоколов;
- применение парольной и антивирусной защиты;
- 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 Университета.

10.5. Запрещается использовать для обработки, передачи и хранения служебной информации публичные облачные сервисы.



11. ТРЕБОВАНИЯ К РАБОТЕ В ККС

11.1. 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;
- установка на рабочем месте сетевых служб без согласования с администраторами ККС или ЛКС, к которой рабочее место подключено;
- разглашение идентификационных данных;
- 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 рассылка электронных сообщений (спам);
- разработка или распространение вредоносного программного обеспечения;
- проведение сетевых атак;
- несанкционированный доступ или попытки несанкционированного доступа к информации;
- использование ККС в личных и коммерческих целях;
- 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.

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

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

11.4. 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.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

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

11.6. В случае необходимости организации больших потоков трафика, в том числе в пределах ККС, во избежание отключения необходимо предварительное согласование с руководством ККС.

12. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

12.1. Отдел мониторинга и контроля качества образования один раз в три года пересматривает данное Положение на соответствие требованиям системы менеджмента.

12.2. По итогам рассмотрения ОМККО может принять решение о продлении действия СТО ПП без изменений. В этом случае действие СТО ПП продлевается на следующие три года, для чего ОМККО делает запись в «Листе регистрации изменений» контрольного экземпляра: «Срок действия продлён до 20__г.», расписывается и ставит дату. В противном случае ОМККО делает запись: «Требуется пересмотра. Срок действия продлён до 202__г. (срок продления в этом случае не должен превышать 1 месяц), расписывается и ставит дату. Такая запись инициирует начало пересмотра данного СТО ПП.

13. СОГЛАСОВАНИЕ, ХРАНЕНИЕ, РАССЫЛКА

13.1. Согласование настоящего Положения осуществляется с проректором по образовательной деятельности и информатизации, начальником отдела правового обеспечения, начальником управления информатизации и оформляется в листе согласования.

13.2. После утверждения Положения ректором первый экземпляр (оригинал) передается на хранение в отдел мониторинга и контроля качества образования (ОМККО), копии в УМУ и структурные подразделения Университета. Ответственность за хранение первого экземпляра (оригинала) Положения несет руководитель ОМККО.

13.3. Копия Положения размещается на официальном сайте Университета.

	Система менеджмента качества СТО ПП-02-02-02-2022
	ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»
	Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

Приложение А

Организация работы беспроводных сетей в ФГБОУ ВО ПГГПУ

1. Беспроводные сети в Университете представлены беспроводными сетями структурных подразделений и публичными беспроводными сетями.
2. Беспроводные сети структурных подразделений являются локальными компьютерными сетями подразделений и должны отвечать требованиям Положения о ККС ПГГПУ.
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 Университете 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.



Приложение Б

Лист регистрации изменений

№ изменения	Номера листов (страниц)			Номер документирования	Подпись	Дата	Срок введения изменения
	новых	Аннулированных	замененных				
1							
2							
3							
4							
5							
6							
7							
8							



Система менеджмента качества СТО ПП-02-02-02-2022

ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет»

Положение о корпоративной компьютерной сети ФГБОУ ВО ПГГПУ

Приложение В

Лист согласования

Ф.И.О.	Должность	Дата	Подпись
Лизунова Л.Р.	Проректор по образовательной деятельности и информатизации		
Отинова А.А.	Начальник отдела правового обеспечения		
Гавриков О.В.	Начальник управления информатизации		