	Министерство образования и науки РФ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р.Е.АЛЕКСЕЕВА» (НГТУ) **Положение по виду деятельности**
НГТУ ПВД 38.1/22-18	Информационно-вычислительный центр

«УТВЕРЖДЕНО»

приказом ректора

от 08.06.2018 № 264

ПОЛОЖЕНИЕ ПО ВИДУ ДЕЯТЕЛЬНОСТИ
«О корпоративной компьютерной сети НГТУ»

НГТУ ПВД 38.1/22-18

«СОГЛАСОВАНО»

Первый проректор

_____ М.В. Ширяев

«07» 06 2018 г.

	Должность	*Фамилия/ Подпись*	*Дата*
Разработал	*Директор ИВЦ*	*И.В.Козин*	04.06.18
Проверил	*Начальник УИ*	*А.М.Лабаев*	04.06.18
Проверил	*Начальник ЮС*	*А.В.Маркеева*	05.06.18
Проверил	*Начальник СКЭиТК*	*П.А.Рындык*	06.06.18

ОГЛАВЛЕНИЕ

1. Область применения

1.1 Положение о корпоративной компьютерной сети НГТУ определяет основные принципы и правила функционирования корпоративной компьютерной сети университета, 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.

2. Нормативные ссылки

ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 23.04.2018).

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.

Приказ ФСТЭК России от 11 февраля 2013 г. №17 (в ред. от 15.02.2017).

ФЗ от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. 01.05.2017).

3. Термины, определения, обозначения и сокращения

3.1 Термины и 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 здания или комплекса зданий 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 Обозначения и сокращения

ИС – информационная система;
ИТ – информационная технология;
ИТС – информационно-телекоммуникационная сеть;
ККС – корпоративная компьютерная сеть;
ЛКС – локальная компьютерная сеть;
УИ – управление информатизации;
ИВЦ – информационно-вычислительный центр.

4. Положения

4.1 Общие положения

4.1.1 Корпоративная компьютерная сеть является технологической основой функционирования ИТ-среды университета, обеспечивающей информационную поддержку учебной, научной и административной деятельности.
4.1.2 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.
4.1.3 ККС представляет собой организационно-технологический комплекс, на основе технологий Ethernet, Wi-Fi 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.

4.1.4 Для объединения территориально удаленных составляющих ККС университета и обеспечения доступа из ККС в глобальную сеть Интернет могут быть использованы каналы связи, арендуемые у операторов связи.

4.1.5 Доступ в ККС предоставляется работникам, обучающимся университета с оборудованных рабочих мест при наличии служебной, учебной необходимости.

4.1.6 Управление ККС и ее развитие осуществляется под руководством первого проректора, управлением информатизации в лице начальника управления и работников информационно-вычислительного центра в соответствии с их должностными инструкциями.

4.2 Основные задачи корпоративной компьютерной сети

4.2.1 ККС университета предназначена для решения следующих основных задач:

- обеспечение информационного взаимодействия структурных подразделений университета, отдельных работников и обучающихся;
- обеспечение надежного, эффективного и безопасного 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.

4.3 Структуру корпоративной компьютерной сети составляют:

- узлы связи университета;
- базовая информационно-телекоммуникационная сеть университета;
- локальные компьютерные сети подразделений;
- беспроводные сети.

4.3.1 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 маршрутизаторы, межсетевые экраны.

4.3.2 Базовая ИТС университета обеспечивает коммутацию и передачу данных между отдельными компонентами ККС. В ее состав входят кабельные линии связи, коммутационное оборудование, а также каналы связи, арендуемые у операторов связи на основании договоров или организованные через общие сети связи, точки подключения рабочих мест.

4.3.3 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.

4.3.4 Беспроводные сети в НГТУ организуются в соответствии с приложением 1 настоящего положения.

4.4 Участниками корпоративной компьютерной сети являются:

- ответственное руководство ККС;
- администраторы ККС университета;
- администраторы ЛКС подразделений;
- администраторы ИС;

- пользователи ККС университета.

4.4.1 Ответственное руководство ККС в составе первого проректора, начальника УИ и директора ИВЦ определяет стратегию развития ККС, требования к ее компонентам с целью обеспечения высокого уровня информатизации университета, а также требования к информационной безопасности.

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

4.4.3 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 противном случае ответственность за функционирование ЛКС возлагается на руководителя подразделения.

4.4.4 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 неназначения администратора ответственность за функционирование ИС возлагается на руководителя подразделения.

4.4.5 Пользователи ККС – работники, обучающиеся и иные лица, использующие сервисы, предоставляемые компонентами ККС университета.

4.5 Права, обязанности и ответственность участников ККС

4.5.1 Права, обязанности и ответственность руководства ККС университета:

4.5.1.1 Обязанности руководства ККС:

- 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 и координацию деятельности администраторов ККС и ИС университета;
- оказывать информационную и техническую помощь администраторам ККС в исполнении их обязанностей;
- Обеспечивать информационную безопасность при работе в ККС.

4.5.1.2 Права руководства ККС:

- осуществлять контроль деятельности администраторов ККС и ИС университета;
- запрашивать отчеты по работе ККС и отдельных ее компонентов;
- издавать обязательные к исполнению участниками ККС распоряжения, 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.

4.5.1.3 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.

4.5.2 Права, обязанности и ответственность администраторов ККС.

4.5.2.1 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, в целях повышения надёжности и безопасности ККС;
- 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;

4.5.2.2 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;
- 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.

4.5.2.3 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.

4.5.3 Права, обязанности и ответственность администраторов ЛКС университета.

4.5.3.1 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.

4.5.3.2 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 законодательства РФ, 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.

4.5.3.3 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.

4.5.4 Права, обязанности и ответственность администраторов ИС университета.

4.5.4.1 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;
- 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.

4.5.4.2 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.

4.5.4.3 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.

4.5.5 Права, обязанности и ответственность пользователей ККС.

4.5.5.1 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.

4.5.5.2 Пользователь имеет право:

- получать доступ к информационным ресурсам ККС в профессиональных, служебных и образовательных 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.

4.5.5.3 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.

4.6 Порядок подключения к корпоративной компьютерной сети

4.6.1 Подключение рабочих мест, локальных компьютерных сетей подразделений, серверов информационных систем к ККС, осуществляется проводным или беспроводным способом и производится работниками информационно-вычислительного центра УИ. Подключение рабочих мест, серверов к локальной компьютерной сети подразделения производится администратором соответствующей ЛКС. Подключение к ЛКС подразделения также может быть осуществлено работниками ИВЦ УИ при согласовании с первым проректором и начальником УИ при наличии оборудования, материалов и технических возможностей.

4.6.2 Подключение к ККС осуществляется на основании служебной записки руководителя подразделения с визой ректора или первого проректора.

4.6.3 На основании служебной записки на подключение к ККС ИВЦ УИ определяет технические условия подключения и составляет техническое предложение. После согласования предложения с начальником УИ и приобретения необходимых оборудования и материалов ИВЦ УИ выполняет работы по монтажу кабельной системы.

4.6.4 При подключении ЛКС к ККС данная ЛКС подразделения подлежит регистрации в УИ. При регистрации определяются состав и структура ЛКС, сетевые настройки для работы в ККС, другие необходимые для подключения параметры, подтверждаемые руководителем подразделения.

4.6.5 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.

4.6.6 Регистрации в УИ подлежат пользователи при получении доступа к сети Интернет через ККС. При регистрации определяются идентификационные данные пользователя, сетевые настройки для работы в ККС, необходимость и ограничения использования сети Интернет, другие параметры, необходимые для подключения.

4.6.7 Регистрация пользователей в ЛКС подразделений или в ИС осуществляется администраторами соответствующих сетей или систем.

4.6.8 Настройка рабочих мест для работы в ККС осуществляется пользователями. В случае использования одного рабочего места несколькими пользователями, настройка осуществляется ответственным лицом, назначаемым распоряжением руководителя этого структурного подразделения. Настройка ЛКС и рабочих мест, подключенных к ЛКС, осуществляется администраторами ЛКС. Настройка ИС осуществляется администраторами ИС. Настройка производится в соответствии с параметрами, определенными при регистрации.

4.7 Безопасность и защита информации в корпоративной компьютерной сети

4.7.1 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.

4.7.2 В соответствии с пунктом 6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждёнными приказом ФСТЭК России от 11 февраля 2013 г. №17), данные Требования целесообразно применять при защите информации, содержащейся в корпоративных информационных системах, в том числе ККС. В связи с этим, в ККС применяются следующие меры защиты информации:

- Идентификация и аутентификация пользователей;
- Идентификация и аутентификация устройств;
- Управление учетными записями и правами доступа пользователей;
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками;
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Регламентация и контроль использования в ККС технологий беспроводного доступа;
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Выявление, анализ уязвимостей ККС и оперативное устранение вновь выявленных уязвимостей;
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- Контроль состава технических средств, программного обеспечения и средств защиты информации;

- Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;
- Периодическое резервное копирование информации на резервные машинные носители информации;
- Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала;
- Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре;
- Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре;
- Регистрация событий безопасности в виртуальной инфраструктуре;
- Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- Контроль целостности виртуальной инфраструктуры и ее конфигураций;
- Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;
- Разбиение ККС на сегменты (сегментирование ККС) и обеспечение защиты сегментов ККС;

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

4.7.4 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.

4.7.5 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.

4.7.6 Запрещается использовать для обработки, передачи и хранения служебной информации личные устройства.

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

4.8 Требования к работе в ККС

4.8.1 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 вредоносногопрограммного обеспечения;
- проведение сетевых атак;
- несанкционированный доступипили 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.

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

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

4.8.4 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.

4.8.5 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.
4.8.6 В случае необходимости организации больших потоков трафика, в том числе в пределах ККС, во избежание отключения необходимо предварительное согласование с руководством ККС.

4.9 Особенности доступа пользователей ККС к сети «Интернет»

4.9.1 Использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области информации.
4.9.2 Пользователи вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законодательством РФ, настоящего положения и другими локальными нормативными актами университета.
4.9.3 Доступ к информации ограничивается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Доступ к информации, распространяемой с нарушением законодательства РФ, запрещён.
4.9.4 Запрещается доступ к информации, причиняющей вред здоровью и (или) развитию детей.
4.9.5 К информации, причиняющей вред здоровью и (или) развитию детей относится:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера;
- о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.
- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

4.10 Доступ к запрещённой информации не допускается без применения административных и организационных мер, технических и программно-аппаратных средств защиты детей от указанной информации.
Ограничение доступа к запрещённой информации осуществляется с учётом, содержащихся на сайтах и аудиовизуальных сервисах в информационно-телекоммуникационной сети "Интернет", предупреждений об ограничении ее распространения среди детей, в соответствии с положениями ст. 14, 15 ФЗ от 29.12.2010 N 436-ФЗ (ред. 01.05.2017) "О защите детей от информации, причиняющей вред их здоровью и развитию", и с помощью системы контент-фильтрации.

Приложение 1

Беспроводные сети в НГТУ

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 НГТУ.
3. Доступ к беспроводным сетям должен быть предоставлен только после проведения идентификации пользователя средствами определёнными действующим законодательством.
4. Беспроводные сети подразделений не являются публичными и должны быть защищены паролем и доступны лишь зарегистрированным пользователям.
5. 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.

6. В случае компрометации либо подозрения на компрометацию пароля необходимо сообщить об этом администратору беспроводной сети. Администратор в свою очередь должен немедленно изменить пароль.
7. При организации беспроводной сети структурного подразделения точки беспроводного доступа должны быть зарегистрированы в УИ.
8. Публичные беспроводные сети в университете организуются УИ.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Дата введения изменения	Номер изменения	Номера разделов, пунктов	Кто разработал (должность, фамилия)	Кто утвердил (должность, фамилия)

Лист ознакомления

№ п/п	Ф.И.О.	Дата	Подпись
1	**2**	**3**	**4**