

ГУАП  
№ 05-86/21  
от 17.03.2021

## ПРИКАЗ



17.03.2021

№ 05-86/21

### Об утверждении положений об официальном сайте ГУАП и корпоративной вычислительной сети ГУАП

В соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», постановлением Правительства Российской Федерации от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации», приказом Федеральной службы по надзору в сфере образования и науки от 14.08.2020 № 831 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети Интернет и формату представления информации» и с целью создания организационной основы функционирования, ведения и информационного наполнения официального сайта ГУАП, организации работ по сопровождению и развитию корпоративной вычислительной сети ГУАП

#### ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:

1.1. Положение об официальном сайте федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (Приложение 1 к настоящему приказу).

1.2. Положение о корпоративной вычислительной сети федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (Приложение 2 к настоящему приказу).

2. В соответствии с Положением о корпоративной вычислительной сети федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» возложить исполнение обязанностей Системного администратора корпоративной вычислительной сети ГУАП на ведущего программиста Центра информационных технологий ГУАП (ЦИТ) Лаврова В.Э.

3. Директору ЦИТ Космачеву В.М. обеспечить работу ЦИТ в соответствии с вышеуказанными положениями.

4. Считать утратившими силу приказ ГУАП от 10.05.2017 № 05-170/17 «Об официальном сайте федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» и Положение о корпоративной сети Санкт-Петербургского государственного университета аэрокосмического приборостроения, утвержденное ректором ГУАП 08.08.2006.

5. Контроль за исполнением настоящего приказа возложить на проректора по учебной деятельности Матьяша В.А.

Ректор

Ю.А. Антохина

Приложение 2  
УТВЕРЖДЕНО  
Приказом ГУАП  
от 17.03.2021 № 05-86/21

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего образования  
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

ПОЛОЖЕНИЕ  
О КОРПОРАТИВНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО  
ПРИБОРОСТРОЕНИЯ»

Положение о корпоративной вычислительной сети федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (далее – ГУАП, Университет) (далее – Положение) является организационной и нормативной основой регулирования принципов и правил функционирования процессов в корпоративной вычислительной сети ГУАП (далее – КВС).

Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 07.07.2003 № 126-ФЗ «О связи», Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», приказом Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», иными нормативными правовыми актами Российской Федерации, уставом ГУАП и локальными нормативными актами ГУАП.

Настоящее Положение определяет задачи и правила функционирования КВС, регламентирует организацию работ по сопровождению и развитию корпоративной сети, определяет организационно-технические мероприятия, направленные на регламентацию работы пользователей и обслуживающего персонала, а также права, обязанности и ответственность пользователей и обслуживающего персонала.

## **1. Общие положения**

1.1. КВС ГУАП является организационным, программно-техническим комплексом и основой единой информационной научно-образовательной среды Университета, главное предназначение которой – реализация задач цифровизации ГУАП и достижение на этой основе качественно нового уровня подготовки специалистов в ГУАП.

1.2. КВС ГУАП является технической и технологической основой эффективного функционирования информационных узлов (серверов), обеспечивающих информационную поддержку научной, методической и преподавательской деятельности работников, включая систему документооборота, а также сферу административного управления.

1.3. КВС ГУАП – это целостная структура вычислительных систем, состоящая из взаимодействующих локальных вычислительных сетей структурных подразделений. Функционирование КВС требует реализации организационно-технических мероприятий, жесткой дисциплины пользователей и служб сопровождения.

1.4. КВС ГУАП является ведомственной корпоративной сетью передачи данных. Доступ в нее предоставляется структурным подразделениям, сотрудникам ГУАП и лицам, обучающимся в ГУАП.

1.5. КВС ГУАП является некоммерческой сетью, то есть извлечение прибыли не является целью эксплуатации сети.

1.6. Для обеспечения доступа к глобальной компьютерной сети Интернет используется отраслевая сеть передачи данных RUNNET, или сети других провайдеров на основании соответствующих договоров.

## 2. Основные задачи

2.1. КВС ГУАП является неотъемлемой частью системы управления и предназначена для решения научно-образовательных задач и задач управления на базе современных информационных технологий, обеспечивающих ускорение принятия решений на основе: оперативного обмена данными между подразделениями, использования общих информационных ресурсов, размещенных в сети, доступа через единую компьютерную сеть к данным других интрасетей и глобальных сетей, использования электронной почты, организации централизованного хранилища данных с различным уровнем доступа к информации, отслеживания изменений данных в реальном масштабе данных.

2.2. Основными задачами формирования и эксплуатации КВС являются: создание, развитие и обеспечение функционирования организационной, технической, программно-методической и технологической информационной инфраструктуры для информационного обеспечения научной, образовательной, методической деятельности, а также административного управления; обеспечение информационного межсетевого взаимодействия в рамках выполняемых проектов.

2.3. КВС ГУАП предназначена для обеспечения:

- информационного взаимодействия подразделений, сотрудников и студентов ГУАП;
- эффективного сбора, обработки, хранения, распространения, поиска, передачи и защиты информации.

- надежного и эффективного доступа к информационным ресурсам на основе соответствующих информационных технологий;

- доступа к глобальной сети Интернет.

2.4. КВС ГУАП предназначена для решения следующих задач:

2.4.1. Создание условий внедрения новых информационно-коммуникационных технологий (далее – ИКТ) и педагогических инноваций на основе ИКТ в основные направления деятельности ГУАП.

2.4.2. Интеграция информационных ресурсов ГУАП на основе ИКТ.

2.4.3. Объединение территориально-распределенных сегментов инфраструктуры Университета.

### **3. Функционально-техническая структура КВС**

3.1. КВС ГУАП это организационно-технологический комплекс, состоящий из следующих функциональных частей:

- средства коммутации;
- серверное оборудование;
- рабочие места на базе персональных компьютеров;
- информационно-вычислительные ресурсы.

3.2. Основными компонентами КВС ГУАП являются центральный телекоммуникационный узел (далее – ЦГУ), расположенный по адресу: Санкт-Петербург, ул. Большая Морская, д. 67, лит. А и сети корпусов, расположенные по адресам: Санкт-Петербург, ул. Большая Морская, д. 67, лит. А; Санкт-Петербург, ул. Гастелло, д. 15, лит. А; Санкт-Петербург, ул. Ленсовета, д. 14, лит. А; Санкт-Петербург, Московский пр., д. 149В, лит. А; Санкт-Петербург, пр. Маршала Жукова, д. 24, лит. А; Санкт-Петербург, ул. Передовиков, д. 13, лит. А; Санкт-Петербург, ул. Варшавская, д. 8, лит. А.

3.3. ЦГУ является основным системно-образующим звеном КВС ГУАП, интегрирующим ресурсы КВС. ЦГУ обеспечивает передачу трафика между локальными вычислительными сетями подразделений (далее – ЛВС подразделений) и КВС ГУАП, а также обеспечивает доступ к глобальной сети Интернет.

3.4. Сети корпусов состоят из магистральных каналов, кабельного, сетевого оборудования и включают в себя ЛВС подразделений ГУАП. Доступ к информационным ресурсам сети ГУАП возможен с использованием беспроводных технологий (wi-fi).

3.5. Информационно-вычислительные ресурсы распределены в КВС ГУАП и доступны в режиме «клиент-сервер». Основные информационные ресурсы сосредоточены

на серверах Центра информационных технологий ГУАП (далее – ЦИТ ГУАП), учебно-научных и административно-организационных подразделений ГУАП.

#### **4. Организация работ по сопровождению и развитию КВС**

4.1. Техническое и организационное управление и эксплуатацию КВС ГУАП осуществляет ЦИТ ГУАП.

4.2. Распоряжением ректора ГУАП назначается системный администратор КВС по представлению директора ЦИТ ГУАП.

4.3. Вопросы, касающиеся функционирования и развития КВС, рассматриваются системным администратором КВС и регламентируются настоящим Положением.

4.4. Подразделения ГУАП вправе организовывать локальные вычислительные сети (ЛВС), входящие в КВС. Создание, ввод в действие и эксплуатация подобных ЛВС осуществляется силами подразделений.

4.5. Для оперативного управления ЛВС, входящих в КВС ГУАП, руководители соответствующих подразделений назначают администраторов ЛВС из числа подготовленных сотрудников.

4.6. Подключение ЛВС подразделений к КВС ГУАП осуществляется по согласованию с ректором и руководителем ЦИТ и выполняется ЦИТ.

4.7. ЦИТ ГУАП осуществляет:

- проектирование, монтаж и программно-техническое сопровождение ЦТУ, сетей корпусов ГУАП;
- технические и оперативные работы по обслуживанию сетей корпусов;
- администрирование адресного пространства;
- мониторинг состояния КВС;
- централизованное распределение и учет адресов ЛВС;
- передачу данных между ЛВС подразделений и другими сетями, включая Интернет;
- обеспечение работы базовых сервисов для IP сетей (сервисы DHCP и DNS);
- ограничение доступа к информационным ресурсам КВС и внешним сетям;
- подключение пользователей АУП и пользователей других структурных подразделений;
- консультации администраторов ЛВС подразделений по вопросам подключения к КВС, по вопросам работы и эксплуатации сетевого программного обеспечения и оборудования.

4.8. Все организационно-нормативные документы разрабатываются ЦИТ ГУАП, согласовываются с Финансово-экономическим управлением и юридическим отделом ГУАП и утверждаются ректором ГУАП.

## **5. Ответственность системного администратора и администраторов ЛВС**

5.1. Системный администратор КВС ГУАП несет ответственность за:

- работоспособность оборудования ЦГУ;
- работоспособность оборудования сетей корпусов;
- информационные ресурсы, расположенные на серверах, закрепленных за ЦИТ ГУАП;
- работу базовых сервисов для IP сетей (маршрутизация, сервисы DHCP и DNS).

5.2. Системный администратор КВС ГУАП не несет ответственности за:

- содержание проходящих по сети данных;
- информацию, находящуюся на компьютерах, входящих в КВС ГУАП;
- установление права доступа к компьютерам в ЛВС и за деятельность, ведущуюся на этих компьютерах;
- работоспособность и техническое состояние линий связи и других средств коммуникаций внутри ЛВС подразделений, эксплуатируемых подразделениями самостоятельно.

5.3. Системный администратор КВС ГУАП пресекает:

- попытки несанкционированного доступа на компьютеры КВС из внешних сетей и с компьютеров ЛВС;
- получение и распространение информации, запрещенной действующим законодательством, регламентом вышестоящей сети, иными нормами, правилами и требованиями, регламентирующими работу в КВС ГУАП.

5.4. Администраторы ЛВС несут ответственность за:

- добросовестное выполнение своих обязанностей, перечисленных в Приложении 1 к настоящему Положению;
- несвоевременное уведомление системного администратора КВС ГУАП об изменениях в маршрутизации и составе подведомственных сетей;
- несвоевременное уведомление системного администратора КВС ГУАП о случаях злоупотреблений в сети, перечисленных в разделе 8 настоящего Положения.

## **6. Порядок подключения к сети**

6.1. Подключение рабочих станций, ЛВС подразделений к КВС ГУАП производится на основании заявки подразделения, подписанной руководителем подразделения, согласованной с указанными в заявке отделами, системным администратором и утвержденной ректором ГУАП. Форма заявки определена в Приложении 2 к настоящему Положению.

6.2. На основании полученной заявки ЦИТ ГУАП определяет технические возможности и условия подключения, дает рекомендации для выполнения подключения к КВС ГУАП.

6.3. После выполнения работ системный администратор КВС ГУАП обновляет информацию о подключенных помещениях, объект подключается к сети и передается подразделению для эксплуатации.

## **7. Безопасность в КВС**

7.1. Политика защиты информации в КВС ГУАП строится ЦИТ ГУАП в соответствии с законодательством Российской Федерации, регламентирующим сферу информационных технологий и защиты информации. Защита представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении ресурсов КВС.

7.2. Организационные мероприятия включают в себя:

7.2.1. Организацию постоянного контроля соблюдения Правил пользования автоматизированными рабочими местами (АРМ), компьютерными классами и вычислительной сетью (ВС) ГУАП.

7.2.2. Проведение антивирусной политики в КВС.

7.2.3. Ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование КВС.

7.2.4. Контроль структуры сети и пресечение несанкционированного подключения компьютерной техники к КВС.

7.2.5. Запрет на использование в сети пелицензионного программного обеспечения.

7.3. Технические мероприятия включают в себя:

7.3.1. Регулярную смену сетевых паролей.

7.3.2. Антивирусный контроль.

7.3.3. Регулярное резервное копирование информации.

7.3.4. Регулярное обновление программного обеспечения.

7.3.4. Физическое выделение сегментов сети, по которым передается конфиденциальная информация.

7.3.5. Отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней и нарушающего безопасность сети.

7.3.6. Логическое выделение компьютеров и/или групп пользователей, обладающих строгим разграничением доступа к разделяемым устройствам.

7.3.7. Ограничение пропуска сетевых протоколов на маршрутизаторах в соответствии с определенными в утвержденных проектах потребностями отдельных сегментов сети.

## **8. Злоупотребления в сети**

8.1. К злоупотреблениям в сети в первую очередь относится деятельность, нарушающая законодательство Российской Федерации в области информации, информационных технологий и защиты информации, а также несанкционированный доступ к КВС ГУАП.

8.2. Несанкционированный доступ к сети определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых компьютерным оборудованием или автоматизированными системами.

8.3. К злоупотреблениям в КВС ГУАП, кроме того, относится:

8.3.1. Доступ к данным и программам лиц, не имеющих на это права;

8.3.2. Уничтожение (или фальсификация) данных и программ без разрешения их собственника;

8.3.3. Незапланированная и необоснованная производственной необходимостью загрузка сети.

8.3.4. Организация VPN соединений за пределы КВС ГУАП без согласования с ЦИТ ГУАП.

8.3.5. Организация внутри КВС ГУАП анонимных прокси-серверов.

8.3.6. Организация внутри КВС ГУАП почтовых серверов без контроля доступа (open-relay).

8.3.7. Использование на рабочих местах каких-либо сетевых адресов, кроме адресов, выданных для этого места системным администратором КВС.

8.3.8. Попытки доступа и доступ к данным и программам, расположенным как внутри КВС ГУАП, так и за ее пределами лиц, не имеющих на это права.

8.3.9. Использование рабочих мест или серверов КВС для осуществления сетевых атак на рабочие станции, сервера и сетевое оборудование КВС, абонентов КВС или любых других сетей Интернет.

#### 8.4. Пресечение злоупотреблений

8.4.1. Администраторы ЛВС обязаны оповестить своих пользователей о содержании настоящего Положения и Правил пользования автоматизированными рабочими местами (АРМ), компьютерными классами и вычислительной сетью (ВС) ГУАП (Приложение 3 к настоящему положению).

8.4.2. Администраторы ЛВС при выявлении злоупотреблений должны информировать ЦИТ ГУАП и немедленно принять меры по пресечению злоупотребления. О принятых мерах следует сообщать в ЦИТ ГУАП и всем заинтересованным службам.

8.5. В случае злоупотребления сетью нарушители частично или полностью отстраняются от пользования сетью и несут ответственность в соответствии с законодательством Российской Федерации.

## **Обязанности администраторов ЛВС**

На администратора ЛВС, входящей в КВС ГУАП, в рамках настоящего Положения возлагаются следующие обязанности:

1. По обеспечению бесперебойной работы серверов и ЛВС:

1.1. Конфигурирование операционной системы на серверах, поддержание в рабочем порядке программного обеспечения сервера.

1.2. Восстановление работоспособности системы после сбоев и выходов из строя сетевого оборудования.

1.3. Выявление причины некорректной работы сетевого оборудования и сетевого ПО.

1.4. Планирование размещения информационных ресурсов, контроль за использованием сетевых информационных ресурсов.

1.5. Обеспечение бесперебойного обмена информацией ЛВС с внешними организациями по телекоммуникационным каналам.

2. По техническому и программному обеспечению технологического процесса в сети:

2.1. Контроль за установкой программного обеспечения на серверах и рабочих станциях.

2.2. Удаление нелегального программного обеспечения с серверов и персональных компьютеров, подключенных к ЛВС.

2.3. Обеспечение интегрирования ПО на серверах и рабочих станциях ЛВС.

2.4. Обеспечение настройки и поддержки информационной системы.

2.5. Подготовка предложений (проектов) по развитию инфраструктуры сети.

2.6. Изучение спроса и подготовка предложений по модернизации и приобретению сетевого оборудования.

2.7. Участие в обустройстве помещений, где планируется организация ЛВС.

3. По организационному сопровождению технологического процесса в сети:

3.1. Организация доступа пользователей к локальной и глобальной сетям.

3.2. Регистрация пользователей, при необходимости назначение идентификаторов и паролей.

3.3. Согласование списка пользователей и прав доступа в сеть с руководителем подразделения, к которому относится ЛВС.

3.4. Разграничение прав доступа пользователей.

3.5. Информирование пользователей ЛВС о порядке работы в сети и ответственности за нарушения, об изменениях в Положении о КВС ГУАП.

4. По ведению системного контроля и анализа состояния системы:

4.1. Осуществление регулярного мониторинга ЛВС.

4.2. Регулярное копирование и резервирование данных.

4.3. Регулярное проведение антивирусных мероприятий.

4.4. Извещение руководителя подразделения обо всех нештатных ситуациях в локальной сети.

4.5. Принятие мер по пресечению несанкционированного доступа к компьютерам и информационным процессам, приводящим к нарушениям нормативных правовых актов Российской Федерации, уведомление ЦИТ ГУАП о случаях нарушений настоящего Положения и принятых мерах.

Приложение 2  
к Положению  
о корпоративной  
вычислительной сети ГУАП

*Форма*

УТВЕРЖДАЮ

Ректор ГУАП

\_\_\_\_\_ Ю.А. Антохина

СОГЛАСОВАНО

Отдел защиты государственной тайны

\_\_\_\_\_ И.В. Савинцева

Комиссия экспортного контроля

\_\_\_\_\_ А.Ф. Крячко

Директор ЦИТ

\_\_\_\_\_ В.М. Космачев

## Заявка на подключение к КВС ГУАП

### 1. Данные сотрудника, ответственного за эксплуатацию сетевого оборудования

Фамилия, имя, отчество: \_\_\_\_\_

\_\_\_\_\_

Подразделение: \_\_\_\_\_

\_\_\_\_\_

Должность: \_\_\_\_\_

Телефон: \_\_\_\_\_

### 2. Описание подключения

Адрес корпуса ГУАП: \_\_\_\_\_

Аудитория: \_\_\_\_\_

Дополнительные сведения о подключаемом оборудовании: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
Наименование должности руководителя  
подразделения

\_\_\_\_\_  
Подпись

\_\_\_\_\_  
Инициалы и Фамилия

**ПРАВИЛА**  
**пользования автоматизированными рабочими местами (АРМ),**  
**компьютерными классами и корпоративной вычислительной сетью**  
**(КВС) ГУАП**

1. При работе с использованием АРМ и ресурсов КВС ГУАП все пользователи обязаны строго соблюдать настоящие правила и следить за их соблюдением другими пользователями.
2. Компьютеры и периферийное оборудование подразделений ГУАП подключаются к КВС при наличии технической возможности и заявки, утвержденной руководителем Университета.
3. Преподаватели и обучающиеся должны использовать АРМ и ресурсы КВС только для работ, относящихся к учебному процессу.
4. Использование информационно-телекоммуникационной сети Интернет и ресурсов КВС сотрудниками допускается только в целях исполнения ими своих должностных обязанностей.
5. Использование информационно-телекоммуникационной сети Интернет и ресурсов КВС обучающимися допускается только в образовательных целях.
6. При использовании ресурсов информационно-телекоммуникационной сети Интернет обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют непосредственное отношение к образовательному процессу.
7. Во время проведения учебных занятий в компьютерных классах, подключенных к КВС, ответственным за соблюдение настоящих правил является преподаватель, ведущий занятия.
8. Во время свободного использования АРМ и КВС обучающимися ГУАП для самоподготовки, ответственным за соблюдение настоящих правил является ответственный за эксплуатацию.
9. Ответственные осуществляют визуальный контроль за содержанием ресурсов, к которым обращаются обучающиеся, и принимают меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.
10. При работе с использованием АРМ и КВС ГУАП студенты обязаны выполнять требования преподавателя и сотрудников, ответственных за эксплуатацию компьютерной техники.
11. В процессе использования обучающимися компьютерной техники работником (преподавателем, ведущим занятие, ответственным работником) осуществляется контроль использования технических средств (программных, программно-аппаратных), в том числе контроль доступа обучающихся к ресурсам сети Интернет.
12. При нарушении правил использования или создания угрозы для безопасности КВС пользователи или структурное подразделение могут быть ограничены в использовании КВС ГУАП.

13. Мониторинг и администрирование сети осуществляется системным администратором КВС ГУАП.

14. Оперативные действия предпринимает системный администратор КВС ГУАП или администраторы локальных подсетей, оповестив об этом соответствующего пользователя или сотрудника подразделения, ответственного за эксплуатацию.

15. К работе с использованием компьютерной техники и КВС допускаются студенты, ознакомленные с настоящими правилами. Нарушение настоящих правил влечет за собой отстранение от работы.

### **ЗАПРЕЩАЕТСЯ:**

1. Включать, отключать, работать за компьютером, подключаться к КВС ГУАП без разрешения преподавателя или ответственного сотрудника.

2. Подключать и отключать любые периферийные устройства, за исключением флеш-накопителей.

3. Прикасаться к соединительным кабелям и их разъемам, к экрану и корпусу монитора, а также изменять местоположение системного блока и монитора.

4. Самостоятельно устранять какие-либо неисправности.

5. Открывать корпус системного блока, монитора, периферийных устройств.

6. Размещать какие-либо предметы (тетради, дискеты, книги и др.) на элементах оборудования АРМ.

7. Продолжать работу при наличии сбоев и неполадок функционирования, нехарактерного шума компьютера или признаков возникновения пожара (запаха гари).

8. Модернизировать или изменять параметры (настройки) операционной системы, сетевые настройки АРМ.

9. Проводить компьютерные атаки, направленные на системы внутри ГУАП или вне его пределов, с целью их перевода в нестабильное состояние.

10. Копировать, уничтожать, фальсифицировать данные или программы, нелегально модифицировать коды программ.

11. Распространять компьютерные вирусы.

12. Осуществлять попытки подбора паролей других пользователей, попытки взлома серверов и систем как внутри ГУАП, так и во внешних сетях.

13. Организовывать доступ к данным и программам для лиц, не имеющих на это права, доступ к КВС ГУАП через машины конечных пользователей или другие устройства.

14. Необоснованно загружать КВС в ущерб другим пользователям.

15. Использовать ресурсы КВС ГУАП в коммерческих или рекламных целях без письменного согласования с руководством Университета.

16. Распространять запрещенные российским законодательством материалы.

17. Неэтичное и недостойное поведение при использовании публичных ресурсов сети Интернет.

18. Другие виды компьютерной активности, реально или потенциально угрожающие нормальному функционированию КВС ГУАП и внешних сетей, а также любая деятельность, противоречащая законодательству Российской Федерации.

### **Перед началом работы**

1. Убедиться в отсутствии видимых повреждений на компьютерах (нарушении целостности корпуса, нарушении изоляции проводов, неисправность индикации включения питания, признаки электрического напряжения на корпусе и т. д.).
2. Начинать работу с компьютером только по указанию ответственного лица.

### **В процессе работы**

1. При непроизвольном отключении ПК, сбоев в работе, нехарактерного шума или запахе гари необходимо немедленно сообщить об этом преподавателю или сотрудникам, ответственным за эксплуатацию компьютерной техники.

### **По окончании работы**

1. Поставить преподавателя в известность об окончании работы с компьютером. Компьютер не выключать!
2. По окончании самостоятельной работы поставить в известность сотрудников, ответственных за эксплуатацию компьютерной техники.