МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Горно-Алтайский государственный университет»
(ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

ПРИЛОЖЕНИЕ №1
к приказу ГАГУ
№164 от 16.06.2026

ИНСТРУКЦИЯ
16.06.2026 № 01-05-65

пользователей и администраторов в федеральном государственном бюджетном образовательном учреждении высшего образования «Горно-Алтайский государственный университет»

Аннотация

Настоящая Инструкция регламентирует работу на автоматизированных рабочих местах (АРМ) в локальной вычислительной сети ФГБОУ ВО ГАГУ (далее – Университет) и использование информационно-телекоммуникационной инфраструктуры (ИТКИ) в целях повышения уровня информационной безопасности. Инструкция обязательна для всех работников структурных подразделений Университета, допущенных к работе с ИТКИ.

Термины и определения

Термин	Определение
УКБ	Управление комплексной безопасности
ИР	Информационные ресурсы
ИС	Информационная система (система электронного документооборота, электронная почта, портал, файловое хранилище и т.п.)
ЦЦР	Центр цифрового развития
ИТКИ	Информационно-телекоммуникационная

	инфраструктура
СВТ	Средства вычислительной техники
АРМ	Автоматизированное рабочее место
ЛВС	Локальная вычислительная сеть
ПО	Программное обеспечение
НСД	Несанкционированный доступ

1. Общие положения

1.1. Доступ к корпоративным информационным системам предоставляется только авторизованным пользователям и исключительно в объёме, необходимом для выполнения должностных обязанностей. Университет управляет предоставлением доступа и контролирует его использование.

1.2. ЛВС – основная составляющая ИТКИ, объединяющая аппаратные и программные средства, среды передачи данных.

1.3. ЛВС предназначена для:

– доступа пользователей к закреплённым АРМ и их использования в служебных целях;

– организации разграниченного доступа к информационным ресурсам;

– подготовки, передачи, хранения и обработки информации;

– коллективного доступа к периферийному оборудованию;

– функционирования корпоративной электронной почты;

– централизованного доступа к сети Интернет;

– обеспечения работы информационных систем.

1.4. В состав ЛВС входят серверы, сетевое оборудование, система управления учётными записями, почтовые серверы, сетевые ресурсы общего и индивидуального доступа, точки доступа в Интернет, прокси-серверы, АРМ администраторов и пользователей, иные аппаратные и программные компоненты.

1.5. Администраторы – лица, ответственные за бесперебойное функционирование ЛВС и предоставление доступа пользователям, – назначаются руководителем ЦЦР из числа штатных сотрудников либо привлекаются по сервисным договорам в рамках их полномочий.

1.6. Предоставление доступа к ЛВС и адреса корпоративной электронной почты осуществляется ЦЦР или уполномоченными представителями подрядчика в установленном в Университете порядке.

1.7. Доступ к Интернету предоставляется исключительно для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам.

1.8. Пользователи обязаны соблюдать настоящую Инструкцию, иные утверждённые регламентирующие документы (Инструкцию по резервному копированию, Регламент антивирусной защиты, Политику парольной защиты), а также следовать рекомендациям сотрудников ЦЦР.

1.9. Инструкция разработана в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» и локальными нормативными актами Университета.

2. Права и обязанности Администратора

2.1. Администратор обладает правами доступа, минимально необходимыми для управления и контроля ИТКИ. Объём прав фиксируется должностной инструкцией.

2.2. Администратор руководствуется настоящей Инструкцией, иными регламентирующими документами Университета.

2.3. Основные обязанности Администратора:

– предоставлять, изменять и прекращать доступ пользователей к ЛВС, электронной почте, сетевым ресурсам и Интернету в соответствии с заявками, оформленными в установленном порядке;

– обеспечивать постоянную работоспособность ИТКИ, контролировать доступность сервисов;

– обеспечивать функционирование средств и систем защиты информации;

– принимать меры реагирования при внештатных и аварийных ситуациях;

– в случае отказа элементов ИТКИ принимать срочные меры по восстановлению;

– при обнаружении признаков НСД или вирусной активности немедленно изолировать АРМ от ЛВС (отключить порт коммутатора или сетевой кабель), зафиксировать наблюдаемые признаки (скриншоты, время, события) и сообщить в ЦЦР и УКБ; запрещается самостоятельно удалять или изменять потенциальные следы инцидента до прибытия специалистов по информационной безопасности;

– вести предусмотренную документацию на ИТКИ, а также при необходимости осуществлять протоколирование действий пользователей в целях обеспечения информационной безопасности в порядке, установленном локальными актами Университета и не противоречащем законодательству РФ;

– настраивать серверное оборудование так, чтобы отклонялись письма, адресованные на не принадлежащие Университету домены, обеспечивать централизованную антивирусную проверку входящей почты.

2.4. Основные права Администратора:

– требовать от пользователей неукоснительного выполнения правил пользования ресурсами ИТКИ;

– временно или постоянно прекращать доступ пользователей к ресурсам в случае нарушения настоящей Инструкции либо по требованию непосредственного руководителя или УКБ.

2.5. Требования Администратора в рамках настоящей Инструкции обязательны для всех пользователей. Действия Администратора могут быть обжалованы руководству ЦЦР.

3. Права и обязанности пользователей

3.1. Пользователь имеет право:

– использовать закреплённое АРМ, корпоративную электронную почту, Интернет, предоставленные сетевые ресурсы и ПО исключительно в служебных целях;

– обращаться в ЦЦР или к уполномоченным сотрудникам подрядных организаций за консультациями по работе АРМ и программных продуктов;

– изменять личные пароли в соответствии с Политикой парольной защиты;

– требовать от ЦЦР обеспечения бесперебойной работы АРМ в рамках установленных процедур.

3.2. Пользователь обязан:

– обладать необходимыми навыками работы с аппаратным и программным обеспечением; выполнять только те процедуры, которые определены должностной инструкцией;

– знать и соблюдать настоящую Инструкцию, а также все регламентирующие документы, упомянутые в п. 1.8;

– использовать исключительно персональные учётные данные; передача идентификационных данных другим лицам категорически запрещена;

– вести служебную переписку только с персонального адреса корпоративной электронной почты;

– контролировать объём отправляемых сообщений (рекомендуемый размер – не более 5 Мбайт);

– следить за исправностью предоставленных технических средств, соблюдать правила их эксплуатации;

– немедленно информировать ЦЦР и УКБ о признаках вирусного заражения, попытках НСД, иных подозрительных событиях;

– при планировании работ, создающих интенсивную нагрузку на ЛВС (передача/получение значительных объёмов данных, большое число соединений), заблаговременно оповещать ЦЦР;

– при оставлении рабочего места блокировать сессию (например, сочетанием клавиш Win+L) для предотвращения несанкционированного доступа.

3.3. Пользователю запрещается:

– устанавливать, модифицировать или хранить любое программное обеспечение без предварительного согласования с ЦЦР;

– самостоятельно разбирать, изменять аппаратную конфигурацию, настройки BIOS/UEFI или загружать АРМ с внешних носителей;

– устанавливать и использовать средства удалённого доступа к АРМ без письменного разрешения руководства УКБ и ЦЦР;

– использовать доступ в Интернет в личных целях, а также для деятельности, противоречащей законодательству РФ, локальным актам Университета или должностной инструкции;

– использовать каналоёмкие ресурсы (файлообменные сети, потоковое видео, онлайн-радио и т.п.) в личных целях; использование таких ресурсов в служебных целях допускается только с согласия ЦЦР;

– изменять параметры и роль предоставленной учётной записи;

– хранить личную информацию на файловых ресурсах ИТКИ;

– хранить или передавать в открытом виде информацию, ограниченную в обороте законодательством РФ или локальными актами (государственная тайна, персональные данные, коммерческая тайна и пр.);

– использовать чужие учётные данные, читать чужую переписку, причинять вред данным других пользователей;

– совершать действия, направленные на обход систем безопасности, статистики, на взлом или сканирование сетевых ресурсов, участвовать в сетевых атаках;

– использовать несуществующие или поддельные обратные адреса при отправке электронных писем;

– размещать на внешних ресурсах от имени Университета сообщения, порочащие честь и достоинство, содержащие оскорбления, угрозы, призывы к насилию или разжиганию розни, а также распространять незаконную, порнографическую или рекламную информацию;

– получать доступ к непубличным информационным ресурсам сети Интернет без разрешения их владельца.

4. Правила работы с корпоративной электронной почтой

4.1. Корпоративная электронная почта предоставляется исключительно для выполнения должностных обязанностей. Использование в личных целях запрещено.

4.2. Все электронные сообщения, создаваемые и хранимые на оборудовании Университета, являются его собственностью. Университет вправе осуществлять контроль (мониторинг) использования электронной почты в порядке, установленном законодательством РФ и локальными актами, в том числе выборочную проверку сообщений для обеспечения соблюдения политики безопасности.

4.3. Пользователь обязан:

– использовать в качестве почтового клиента только утверждённое ЦЦР программное обеспечение;

– перед открытием проверять все входящие вложения и ссылки (запрещено открывать вложения с расширениями .exe, .scr, .bat, .cmd, .js, .vbs и т.п. от незнакомых или не вызывающих доверия отправителей);

– не пересылать защищённую информацию без применения разрешённых криптографических или организационных мер защиты.

4.4. Пользователю запрещается:

– производить массовые или не согласованные предварительно рассылки (спам);

– отправлять письма от имени других пользователей;

– предоставлять доступ к своему почтовому ящику посторонним лицам.

5. Правила использования веб-ресурсов

5.1. Поиск и использование информации в сети Интернет разрешены только в рамках служебных задач.

5.2. Пользователь обязан:

– все загружаемые из Интернета файлы немедленно проверять антивирусным средством;

– избегать переходов по рекламным баннерам и подозрительным ссылкам (особенно ведущим к исполняемым файлам);

– воздерживаться от посещения неблагонадёжных и нелегальных сайтов.

5.3. Запрещается:

– загружать или устанавливать нелицензионное программное обеспечение;

– работать при отключённых штатных средствах защиты (антивирус, межсетевой экран и др.);

– передавать защищаемую информацию способами, не предусмотренными политикой безопасности организации;

– получать доступ к ресурсам, не являющимся публичными, без разрешения их собственника.

6. Рекомендации и ограничения общего характера

6.1. Пароли:

– запрещается записывать пароли на бумаге, в файлах, наклейках и любых других доступных посторонним носителях;

– запрещается сообщать личный пароль другим лицам и регистрировать их в системе под своим паролем.

6.2. Электронная почта и гиперссылки:

– не открывать вложения, если нет уверенности в отправителе;

– с осторожностью переходить по гиперссылкам в письмах.

6.3. Общие правила:

– не осуществлять действия, ведущие к нарушению штатной работы ИТКИ;

– соблюдать исходный уровень защищённости при работе с конфиденциальными документами (зашифрованное письмо нельзя пересылать в открытом виде);

– уважать права других пользователей, не допускать порчи или фальсификации чужой информации.

7. Порядок действий при утере пароля или компрометации учётной записи

7.1. При утрате пароля пользователь обязан немедленно восстановить доступ:

– самостоятельно через форму восстановления, либо путём обращения в ЦЦР для сброса и установки нового пароля.

7.2. При подозрении на компрометацию учётной записи (действия от чужого имени, несанкционированный доступ) пользователь обязан:

– немедленно уведомить ЦЦР и УКБ;

– не выполнять никаких действий с учётной записью до указаний администратора.

7.3. Администратор обязан незамедлительно заблокировать скомпрометированную учётную запись и инициировать служебное расследование.

8. Ответственность

8.1. Пользователь несёт персональную ответственность за:

– сохранность и надлежащую эксплуатацию закреплённого АРМ и установленного ПО;

– все действия, совершённые от его имени с использованием выданных идентификационных данных;

– информационный обмен, инициированный с его АРМ;

– сохранность информации, хранящейся на его АРМ (в пределах предоставленных прав).

8.2. Нарушение требований настоящей Инструкции влечёт:

– отстранение от работы с ресурсами ИТКИ (по решению ЦЦР или УКБ);

– дисциплинарную, административную или уголовную ответственность в соответствии с законодательством РФ, если нарушение повлекло уничтожение, блокирование, модификацию, копирование охраняемой информации либо нарушение работы ИТКИ.

8.3. Обо всех фактах нарушения Инструкции пользователь обязан незамедлительно сообщать непосредственному руководителю, в ЦЦР или УКБ.