

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Куижева Саида Казбековна
Должность: Ректор
Дата подписания: 30.09.2026 09:34:52
Уникальный программный идентификатор:
71183e1134ef9cfa69b206d480271b3c1a975e6f

МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МАЙКОПСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «МГТУ»)**

ПРИКАЗ

06.06.2022

№ 251/1

**Об ответственности за защиту информации в
ФГБОУ ВО «МГТУ»**

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях реализации мер, предусмотренных приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить администратором информационной безопасности в ФГБОУ ВО «МГТУ» проректора по цифровизации Игнатову Дмитрия Алексеевича.
2. Утвердить:
Инструкцию администратора информационной безопасности ФГБОУ ВО «МГТУ» (приложение № 1).
Инструкцию пользователя информационных систем в ФГБОУ ВО «МГТУ» (приложение № 2).
3. Контроль за выполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

Ректор



С.К. Куижева

ИНСТРУКЦИЯ

администратора информационной безопасности в ФГБОУ ВО «МГТУ»

1. Общие положения

Администратор информационной безопасности назначается приказом ректора ФГБОУ ВО «МГТУ». Администратор информационной безопасности руководствуется требованиями нормативных документов Российской Федерации, нормативных актов ФГБОУ ВО «МГТУ», настоящей инструкцией администратора информационной безопасности в ФГБОУ ВО «МГТУ» (далее – Инструкция), а также другими распорядительными документами в части, его касающейся.

Администратор информационной безопасности в пределах своих функциональных обязанностей обеспечивает работоспособность информационных систем (далее – ИС), безопасность персональных данных, обрабатываемых, передаваемых и хранимых при помощи средств вычислительной техники (далее – СВТ) в ИС ФГБОУ ВО «МГТУ».

Должностные лица ФГБОУ ВО «МГТУ», задействованные в обеспечении функционирования ИС, могут быть ознакомлены с основными положениями Инструкции в части, их касающейся, по мере необходимости.

В случае увольнения администратор информационной безопасности обязан передать ответственному за организацию обработки персональных данных и ответственному за защиту информации в ФГБОУ ВО «МГТУ» все носители защищаемой информации (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им должностных обязанностей во время работы в ФГБОУ ВО «МГТУ».

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

- обеспечивать работоспособность СВТ ИС ФГБОУ ВО «МГТУ», проводить организационно-технические мероприятия по их обслуживанию;
- устанавливать и настраивать элементы ИС и средства защиты информации (далее – СЗИ), а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;
- рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИС ФГБОУ ВО «МГТУ»;
- выполнять резервное копирование и восстановление данных;
- обеспечивать контроль выполнения пользователями требований «Инструкции пользователя ИС в ФГБОУ ВО «МГТУ»;

- осуществлять контроль работы пользователей ИС, выявлять попытки несанкционированного доступа к защищаемым информационным ресурсам и техническим средствам ИС ФГБОУ ВО «МГТУ»;
- осуществлять настройку СЗИ, выполнять другие действия по изменению элементов ИС;
- осуществлять учет всех защищаемых машинных носителей информации с помощью их любой маркировки и с занесением учетных данных в соответствующий журнал. Учетные носители информации выдавать пользователям под подпись;
- осуществлять текущий и периодический контроль работы средств и систем защиты информации;
- осуществлять текущий контроль технологического процесса обработки защищаемой информации;
- участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;
- участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;
- проводить обучение работников и пользователей ИС правилам работы с СВТ и СЗИ;
- участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением СЗИ, выполнением мероприятий по обеспечению защиты информации;
- регулярно анализировать работу любых элементов систем, электронных системных журналов, средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования.

3. Права администратора информационной безопасности

Администратор информационной безопасности имеет право:

- отключать любые элементы системы защиты персональных данных при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;
- в установленном порядке изменять конфигурацию элементов ИС;
- требовать от работников ФГБОУ ВО «МГТУ» соблюдения правил работы в ИС, приведенных в «Инструкции пользователя информационных систем в ФГБОУ ВО «МГТУ»;
- требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов ФГБОУ ВО «МГТУ», регламентирующих вопросы обеспечения безопасности и защиты информации;
- вносить свои предложения по совершенствованию функционирования ИС ФГБОУ ВО «МГТУ»;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИС ФГБОУ ВО «МГТУ».

4. Ответственность администратора информационной безопасности

Администратор информационной безопасности несет ответственность за:

- ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими инструктивными документами в соответствии с действующим трудовым законодательством Российской Федерации;

- полноту и качество проводимых им работ по обеспечению защиты информации;

- правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

- разглашение персональных данных в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

На администратора информационной безопасности возлагается персональная ответственность за работоспособность и надлежащее функционирование средств обработки персональных данных в ИС и СЗИ ФГБОУ ВО «МГТУ».

ИНСТРУКЦИЯ

пользователя информационных систем в ФГБОУ ВО «МГТУ»

1. Общие положения

Ознакомление работников ФГБОУ ВО «МГТУ» с требованиями настоящей инструкции пользователя информационных систем (далее – Инструкция) проводит администратор информационной безопасности с выдачей электронных копий Инструкции непосредственно для повседневного использования в работе.

2. Функции и обязанности пользователей информационных систем

Каждый работник ФГБОУ ВО «МГТУ», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки защищаемой информации (персональных данных) и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы (далее – ИС), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;
- выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;
- знать и строго выполнять правила работы со средствами защиты информации, установленными в ИС;
- хранить в секрете свои рабочие пароли;
- немедленно ставить в известность администратора информационной безопасности и руководителя структурного подразделения в случае утери личных реквизитов доступа, при компрометации личных паролей, подозрении на совершение попыток несанкционированного доступа к персональным электронно-вычислительным машинам (далее – ПЭВМ), обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИС;
- немедленно ставить в известность администратора информационной безопасности при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИС, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных технических средств защиты информации;
- при обработке на ПЭВМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию

закрепленной за ним ПЭВМ в структурном подразделении;

- при обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители.

Пользователям ИС запрещается:

- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

- хранить и обрабатывать личную информацию на ПЭВМ и серверах ИС;

- при работе в сети Интернет:

- а) использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

- б) использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;

- в) использовать информационные ресурсы сети Интернет в личных целях;

- г) вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства;

- оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от несанкционированного доступа;

- оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;

- оставлять без личного присмотра в легкодоступном месте, на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения;

- использовать в работе неучтенные носители информации для обработки защищаемой информации;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, об обнаружении такого рода ошибок – ставить в известность администратора информационной безопасности и руководителя своего структурного подразделения.