

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ПРИКАЗ

27.02.2025

№ 175-ОД

Об утверждении регламента
безопасной работы пользователей
в информационных системах

С целью защиты информации от несанкционированного нарушения её конфиденциальности, целостности и доступности в системах федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет»

ПРИКАЗЫВАЮ:

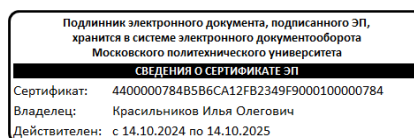
1. Утвердить и ввести в действие с 20.02.2025 регламент безопасной работы пользователей в информационных системах Московского политехнического университета (далее – Регламент) (Приложение к настоящему приказу).

2. Руководителям структурных подразделений обязать руководствоваться Регламентом всех работников, использующих ресурсы информационных систем университета.

3. Отделу контроля и делопроизводства (О.В. Макарова) обеспечить рассылку настоящего приказа и приложения к нему руководителям всех структурных подразделений.

4. Контроль за исполнением приказа возложить на начальника центра информационных технологий А.В. Панферова.

Проректор
по цифровому развитию



И.О. Красильников

Приложение

УТВЕРЖДЕН

приказом Московского Политеха

от « 27 » февраля 2025 г. № 175-ОД

РЕГЛАМЕНТ

**безопасной работы пользователей в информационных системах
Московского политехнического университета**

г. Москва, 2025 г.

1. Область применения

1.1 Регламент безопасной работы пользователей в информационных системах Московского политехнического университета (далее – Регламент) определяет порядок работы сотрудников с ресурсами и сервисами локально-вычислительных сетей Московского политехнического университета (далее – Университет).

1.2 Настоящий Регламент является дополнением к действующим нормативным документам, определяющим требования режима и информационной безопасности.

1.3 Регламент предназначен для применения всеми работниками, во всех структурных подразделениях, использующих ресурсы информационных систем университета.

1.4 Внесение изменений в настоящий Регламент производится при изменении законодательства Российской Федерации и утверждении локальных нормативных и организационных документов, регламентирующих работу с локальными вычислительными сетями.

2. Нормативная база

Настоящий регламент разработан в соответствии с:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
- Федеральный закон от 29 июля 2004 г. № 98 «О коммерческой тайне».

3. Термины и определения

В настоящем Регламенте применены следующие термины с соответствующими определениями:

3.1 Авторизация: предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий;

3.2 Локальная вычислительная сеть: вычислительная сеть, охватывающая небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных;

3.3 Обладатель информации: лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

3.4 Сетевой ресурс: устройство или часть информации, к которой может быть осуществлен удаленный доступ с другого компьютера, обычно через локальную вычислительную сеть;

3.5 Учетная запись (аккаунт): хранимая в компьютерной системе совокупность данных о пользователе;

3.6 Персональные данные: любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

4. Обозначения и сокращения

В настоящем Регламенте применены следующие обозначения и сокращения:

- ИБ – информационная безопасность;
- ИТ – информационные технологии;
- ЛВС – локальная вычислительная сеть;
- ПК – персональный компьютер;
- ПО – программное обеспечение;
- ПДн – персональные данные;
- ООД – окончное оборудование данных;
- ЭП – электронная подпись;
- ИС – информационная система или сервис (например, 1С, электронная почта и т.п.).

5. Общие положения

5.1 В соответствии с п. 1 ч. 3 ст. 6 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» обладатель информации имеет право разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

5.2 В соответствии с ч. 1 ст. 6 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», обладателем (владельцем) информации в ЛВС является Университет.

5.3 ЛВС является средством для передачи и хранения информации производственного характера, обрабатываемой в процессе повседневной деятельности работников.

5.4 ЛВС служит для:

- повышения эффективности деятельности структурных подразделений;
- обмена информацией внутри Университета;
- работы в составе информационных систем;

5.5 К средствам ЛВС относятся:

- физические линии передачи данных – проводные средства (витая пара, волоконно-оптический кабель);

- сетевые контроллеры (адаптеры, сетевые карты);
- коммутирующие устройства;
- концентраторы оконечных систем – для подключения нескольких ООД;
- коннекторы – для механического и непосредственного электрического подключения узлов к кабелю.

5.6 Действия со средствами ЛВС на сетевых ресурсах – сетевых дисках и папках (запись и удаление информации) производит пользователь. Пользователь несет персональную ответственность за размещение информации и работе с ресурсами ЛВС. Работники получают доступ к работе с ЛВС после ознакомления с положениями настоящего Регламента.

5.7 С целью защиты информации от несанкционированного нарушения её конфиденциальности, целостности и доступности в системах Университета организационными и техническими средствами реализована система защиты информации.

5.8 К работе с информационными системами Университета допущены системные администраторы, специалисты по информационной безопасности (далее – Администраторы), а также пользователи информационных систем (далее – Пользователи). В Университете назначен ответственный за организацию обработки персональных данных.

5.9 Пользователи информационных систем при работе с техническими средствами и информационными технологиями, являющимися частью ЛВС должны соблюдать положения настоящего Регламента. Данный регламент распространяется как на пользователей, работающих в очном формате, так и на пользователей, работающих в удаленном режиме доступа.

5.10 Пользователи ЛВС не являются привилегированными пользователями информационных систем ЛВС. Каждому пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам Университета.

5.11 В соответствии с частью 4 статьи 10 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» в ЛВС Университета применяются средства мониторинга и методы технической защиты конфиденциальной информации.

5.12 Выполнение работниками требований настоящего Регламента контролируется сотрудниками отдела развития информационных сетей с применением средств управления, контентной фильтрации и технической защиты информации, а также средств управления и технической защиты ЛВС.

6. Обязанности администраторов и специалистов по защите информации по управлению информационной безопасностью в информационных системах Университета

6.1 Создание и поддержание ЛВС в работоспособном состоянии обеспечивает отдел развития информационных сетей.

6.2 Работниками отдела развития информационных сетей, в целях передачи и хранения информации в ЛВС, создаются сетевые ресурсы – сетевые диски и папки.

6.3 Удаленный доступ работников к сетевым ресурсам, назначение прав доступа к сетевым дискам и папкам обеспечивается работниками Центра информационных технологий, отделом развития информационных сетей и отделом развития информационной инфраструктуры.

6.4 Изменение конфигурации ПО групп пользователей, настройка сетевого доступа работников проводится только сотрудниками отдела развития информационных сетей.

7. Обязанности пользователя по защите информации в информационных системах Университета

7.1 Пользователь информационных систем Университета обязуется выполнять только те действия, которые необходимы для выполнения его служебных обязанностей. Любые посторонние действия в ИС и ЛВС запрещены.

7.2 Пользователь незамедлительно оповещает Администраторов о любой подозрительной активности в ИС.

7.3 Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для несанкционированного копирования, фотографирования, распространения и передачи защищаемой информации.

7.4 Пользователю запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

7.5 Пользователю запрещено изменение источника загрузки своего автоматизированного рабочего места (далее – АРМ) и загрузка АРМ с внешних носителей.

7.6 В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, Пользователь должен блокировать сеанс пользователя АРМ при покидании рабочего места.

7.7 Антивирусная защита в Университете реализована прозрачно для пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится Администраторами централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать Администратора о локальных сообщениях антивирусного программного обеспечения на его АРМ. Пользователь должен оповещать Администратора о любых аномалиях в работе АРМ.

7.8 Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных обязанностей. Установка разрешенного программного обеспечения осуществляется отделом технической поддержки Университета. Также к установке и настройке программного обеспечения, при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

7.9 Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ИС, ключевой информации и к любой другой защищаемой информации. Пользователь незамедлительно сообщает Администратору о подобных попытках (как удачных, так и неудачных).

7.10 Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

7.11 Пользователь должен знать и соблюдать положения настоящего Регламента, внутренних нормативных документов Университета, нормативных документов, указанных в п.2 настоящего Регламента. При возникновении у Пользователя вопросов по защите информации и защите персональных данных в Университете, он обращается к Администратору. Новые Пользователи ИС перед началом выполнения своих служебных обязанностей должны быть ознакомлены с настоящим Регламентом.

8. Правила получения и управления парольной и парольно-ключевой информацией

8.1 Пользователь перед началом работы в ИС получает учетные данные (логин, пароль) в Центре информационных технологий. Учетные данные выдаются Пользователю на основании заявки в системе Bitrix24, служебной записки руководителя подразделения в соответствии с должностной инструкцией.

8.2 Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (в отдельных файлах, в внешних системах хранения, браузерах, на листах бумаги, в незапираемой тумбе, под клавиатурой, на мониторе и т.п.).

8.3 Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

8.4 Пользователю запрещено разглашать другим пользователям свой пароль, в том числе Администратору.

8.5 Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ИС другим Пользователями или посторонним лицам, поскольку все выполненные этими лицами действия в ИС будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

8.6 Пользователю запрещено оставлять без присмотра персональные токены для хранения ЭП.

8.7 Пользователю запрещено передавать сертификат электронной подписи другим Пользователям и посторонним лицам, поскольку все выполненные этими лицами действия в ИС и внешних системах с использованием ЭП будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

9. Правила работы с корпоративной электронной почтой

9.1 Пользователь перед началом работы в ИС получает учетные данные (логин, пароль) в Центре информационных технологий. Учетные данные выдаются Пользователю на основании заявки в системе Bitrix24, служебной записки руководителя подразделения в соответствии с должностной инструкцией.

9.2 Пользователю запрещается использовать корпоративную электронную почту для регистрации на порталах, не относящихся к служебной деятельности и выполнению служебных задач.

9.3 При получении подозрительных писем пользователь обязуется сообщить об этом Администраторам. При получении подозрительных писем для последующего добавления Администраторами мошеннического адреса в черный список требуется переслать письмо на специальный адрес: spam-report@mospolytech.ru.

9.4 Пользователю запрещается скачивать файлы или переходить по ссылкам, содержащимся в подозрительных письмах, поскольку все последствия таких действий, будут считаться последствиями действий, выполненных Пользователем. Ответственность за указанные действия несет Пользователь.

9.5 В случае подозрения Пользователя на применение против него методов социальной инженерии с помощью электронной почты, Пользователь незамедлительно сообщает о данном факте Администратору.

10. Правила работы с съемными носителями информации

10.1 Пользователю при работе с ИС разрешается использовать только выданные Университетом съемные носители информации (флеш-носители, съемные жесткие диски, карты памяти и пр.).

10.2 При необходимости выноса съемного носителя из помещения, Пользователь обеспечивает защиту съемного носителя от утери, кражи или компрометации защищаемой информации на этом носителе.

10.3 В случае утери или кражи съемного носителя информации, Пользователь оперативно сообщает об этом Администратору.

10.4 Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.

10.5 Пользователь несет ответственность за заражение съемных носителей информации вирусом, если он не предпринял необходимых мер для защиты своих данных и устройств. Это включает в себя использование антивирусного программного обеспечения и соблюдение правил безопасности при подключении съемных носителей информации к компьютерам.

10.6 Подключение съемных носителей информации к непроверенным или общественным компьютерам с последующим использованием съемных носителей информации в ЛВС или на компьютерах университета запрещено.

10.7 Пользователи должны осознавать свою ответственность за сохранность информации на флеш-носителях. Это включает в себя регулярное сканирование устройств на наличие вирусов и отказ от подключения флеш-носителей к компьютерам с подозрительной активностью.

11. Ответственность

Пользователь несет ответственность за:

- действия, повлекшие несанкционированный доступ, несанкционированное копирование, модификацию и блокирование или уничтожение информации;
- разглашение сведений, составляющих служебную и коммерческую тайну, другую конфиденциальную информацию, ставших известными ему в связи с исполнением своих должностных обязанностей;
- сокрытие факта несанкционированного доступа, несанкционированного копирования, модификации и блокирования или уничтожения информации вследствие прямых, или косвенных действий пользователя ИС;
- утерю средств хранения информации.

12. Контроль использования удаленного защищенного доступа к ЛВС

12.1 Контроль действий пользователей в ЛВС осуществляют подразделения центра информационных технологий, ответственные за администрирование сети и информационную безопасность.

12.2 При выявлении нарушений требований настоящего Регламента работники центра информационных технологий докладывают об обнаруженных нарушениях руководителю центра или проректору по цифровому развитию.

12.3 По фактам нарушений требований настоящего Регламента, на основании соответствующего распорядительного документа может быть проведено служебное расследование (проверка).

12.4 Работники, нарушившие требования настоящего Регламента, могут быть привлечены к дисциплинарной ответственности в порядке, установленном действующим законодательством и локальными нормативными актами Университета.