МИНОБРНАУКИ РОССИИ

Федеральное государственное
бюджетное образовательное учреждение
высшего образования
**Российский государственный
гуманитарный университет
(ФГБОУ ВО «РГГУ»)**

УТВЕРЖДАЮ

Ректор РГГУ

А.Б. Безбородов

«09» декабря 2022 г.

Политика информационной безопасности

1. Общие положения

Политика информационной безопасности (далее Политика) распространяется на все структурные подразделения РГГУ и обязательна к исполнению всеми ее работниками.

Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах РГГУ, а также в договорах.

1.1. Политика информационной безопасности РГГУ - это комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в РГГУ для обеспечения информационной безопасности (ИБ).

1.2. Цели и задачи настоящей Политики.

1.2.1. Основными целями защиты информации РГГУ являются:

- повышение стабильности функционирования РГГУ в целом;
- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение или снижение ущерба от инцидентов ИБ.

1.2.2. Основными задачами деятельности по обеспечению ИБ являются:

- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ с учетом законодательных требований;
- разработка и совершенствование регламентирующих документов РГГУ в области обеспечения ИБ;
- выявление, оценка и прогнозирование угроз ИБ;
- выработка рекомендаций по устранению уязвимостей;
- организация антивирусной защиты информационных активов;
- защита информации от НСД и утечки по техническим каналам связи.

810

2. Основные принципы обеспечения безопасности

Основными принципами обеспечения ИБ являются следующие:

- постоянный и всесторонний анализ информационных систем с целью выявления их уязвимостей;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер, адекватных характеру выявленных угроз;
- контроль эффективности принимаемых защитных мер;
- персонификация, разделение ролей и ответственности между работниками, исходя из принципа персональной ответственности за совершаемые операции.

3. Требования по обеспечению информационной безопасности

Комплекс мер по обеспечению ИБ предусматривает:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации документов;
- минимально необходимый, гарантированный доступ работника Университета только к тем ресурсам информационного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;
- контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;
- аутентификацию обрабатываемой информации;
- восстановление информации в случае ее умышленного или случайного разрушения (искажения) или выхода из строя средств вычислительной техники;
- гарантированную доставку сообщений участникам информационного обмена.

3.1.Требования по обеспечению ИБ на всех стадиях жизненного цикла информационных систем РГГУ

Информационная безопасность должна обеспечиваться на всех стадиях технологических процессов, с учетом всех сторон, вовлеченных в процессы жизненного цикла: разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений РГГУ.

Ввод в действие и снятие с эксплуатации систем защиты осуществляются при участии работников ответственных за информационную безопасность.

Все объекты, критичные с точки зрения ИБ, т.е. сервера, маршрутизаторы и другие электронные устройства, находятся в охраняемых и контролируемых помещениях.

При неавтоматизированной обработке информации конфиденциального характера (личные дела сотрудников, студентов, абитуриентов и др.) документы должны храниться в шкафах, исключаемых несанкционированный доступ к ним. (Инструкция по делопроизводству РГГУ, от 25.05.2019 г.)

3.2. Требования по обеспечению ИБ при управлении доступом и регистрации

Все работы, связанные с производством и передачей информации, выполняются в соответствии с официальными должностными обязанностями работников, соблюдением требований работы в локальной сети РГГУ и с использованием защищенных каналов связи при взаимодействии с внешними информационными сетями:

- работники РГГУ, а также лица, принимаемые на работу по договорам гражданско-правового характера, подписывают обязательство о неразглашении конфиденциальной информации;
- права доступа работников к персональным данным распределяются в соответствии с действующими положениями РГГУ «Политика в области обработки и защиты персональных данных, от 31.01.2022 г.» и «Положение об обеспечении безопасности при обработке персональных данных, от 31.01.2022 г.»;
- в составе автоматизированных систем требуется использовать сертифицированные или разрешенные к применению средства защиты информации от НСД;
- авторизация, контроль и управление доступом к информационным активам, в том числе функционирование системы парольной защиты, осуществляются в соответствии с Инструкцией для служебного пользования «Мониторинг информационной безопасности и антивирусного контроля при обработке данных в РГГУ»;
- регистрация действий работников и пользователей производится в журналах событий системного программного обеспечения. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий;
- при взаимодействии с внешними информационными сетями используются защищенные каналы связи: взаимодействие с суперсервисом «Поступление в ВУЗ онлайн», с ФЦТ, с ГИС СЦОС, с Рособрнадзором, с ЕИС ГА, с Пенсионным фондом и с Минобрнауки России.

3.3. Требования по обеспечению ИБ по работе в локальной сети РГГУ

Доступ сотрудников к работе в информационных системах осуществляется в соответствии с их должностными обязанностями. Регистрация выполняется системным администратором в соответствии с правами доступа сотрудников РГГУ к внутренним и внешним электронным информационным ресурсам.

Мониторинг информационной безопасности автоматизированных систем от несанкционированного доступа, распространения, искажения и утраты информации, осуществляет Управление по информатизации и информационным технологиям УИИТ.

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств.

Требования к пользователям:

- при работе не использовать без необходимости потенциально опасные ресурсы сети Интернет (социальные сети, ICQ-приложения и т.п.);
- не устанавливать самостоятельно на компьютеры программное обеспечение и приложения, позволяющие осуществлять удаленный доступ к этому компьютеру (Team Viewer, Радмин и т.п.);
- при работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей;
- исключить возможность установки посторонними лицами (посетителями, студентами) на компьютер «шпионских» программ.

На рабочих местах пользователей и на серверах установлено антивирусное программное обеспечение с регулярным централизованным обновлением баз.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.).

При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

Для обмена электронными документами используются усиленные квалифицированные электронные подписи. Состав должностных лиц и работников – владельцев ЭЦП определяет ректор РГГУ. (Инструкция по делопроизводству РГГУ, от 25.05.2019 г.).

Ответственность за все действия в сети, произведенные под именем и с паролем пользователя им самим или другими лицами, полностью лежит на самом пользователе. РГГУ не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение настоящих требований.

3.4. Требования по обеспечению ИБ в сети Интернет

Руководство РГГУ оставляет за собой право в целях обеспечения ИБ производить выборочные и полные проверки всей системы и отдельных файлов без предварительного уведомления студентов и работников.

Пользователям **запрещается**:

- посещение ресурсов с непристойным содержанием (эротико-порнографические, нацистские или националистические, призывающие к насилию и т.п.);
- использование электронной почты и досок объявлений на компьютерах РГГУ в личных целях;
- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;
- передача конфиденциальной информации третьей стороне;
- подключение к электронной сети под другим логином и паролем;
- нанесение вреда электронной системе РГГУ;
- проведение незаконных операций в глобальной сети Интернет;
- создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя;
- любые попытки деструктивных действий по отношению к нормальной работе электронной системы РГГУ и сети Интернет (рассылка вирусов, ip-атаки и т.п.);
- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;
- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения;
- осуществление попыток несанкционированного доступа к ресурсам сети, проведение или участие в сетевых атаках и сетевом взломе;
- совершение действий, противоречащих законодательству РФ, а также настоящим требованиям.

Лица, нарушающие требования работы в локальной сети и в сети Интернет могут быть лишены права пользования сетями РГГУ и несут административную ответственность.

Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.