МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Россчйской Федерации

П Р И К А З

17 МАЙ 2024 № 268

Ростов-на-Дону

Об утверждении Положения об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

В соответствии с Указом Президента Российской Федерации № 250 от 01.05.2022 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», а также в целях обеспечения защиты информации и персональных данных в информационных сетях ФГБОУ ВО РостГМУ Минздрава России, и на основании решения ученого совета от 14.05.2024 года, протокол № 5, п р и к а з ы в а ю:

1. Утвердить Положение об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России (далее Положение) (Приложение 1).
2. Габуния А.Ю., начальнику департамента комплексной безопасности, разместить Положение на официальном сайте ФГБОУ ВО РостГМУ Минздрава России.
3. Руководителям всех структурных подразделений ФГБОУ ВО РостГМУ Минздрава России обеспечить соблюдение требований Положения подчиненными работниками.
4. Считать утратившим силу «Положение об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России», утвержденное приказом от 22.06.2022 № 388.
5. Ответственность за исполнение приказа возложить на Кандыбу В.Н., проректора по безопасности.
6. Контроль исполнения приказа оставляю за собой.

Ректор С.В. Шлык

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

ВЫПИСКА ИЗ ПРОТОКОЛА

заседания ученого совета

«14» мая 2024г. № 5

г. Ростов-на-Дону

Председатель ученого совета, профессор Шлык С.В.

Ученый секретарь ученого совета, профессор Сапронова Н.Г.

Состав совета 54 человека.

Присутствовали 51 человек.

Слушали: об утверждении Положения об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России.

Постановили: утвердить Положение об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России.

Подлинный протокол №5 от 14.05.2024г. подписан председателем ученого совета, профессором Шлык С.В. и ученым секретарем ученого совета, профессором Сапроновой Н.Г.

Выписка верна.

Ученый секретарь ученого совета РостГМУ,
профессор Н.Г. Сапронова

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИНЯТО
на заседании ученого совета
ФГБОУ ВО РостГМУ Минздрава России
Протокол № 5 от 14 МАЙ 2024

УТВЕРЖДЕНО
приказом ректора
от 17 МАЙ 2024 № 268

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФГБОУ ВО РостГМУ МИНЗДРАВА РОССИИ

№ 24-268

2024 г.

Термины и определения

ИБ – информационная безопасность.
ИС – информационная система.
ОС – операционная система.
ИСПДн – информационная система персональных данных.
БД – база данных.
ЭП – электронная подпись.
ЛВС – локальная вычислительная сеть.

Конфиденциальная информация – информация, доступная только субъекту доступа, имеющего на него право.

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационных систем РостГМУ.

Автоматизированное рабочее место (АРМ) – это рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации.

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи, обработки данных, информации и производства вычислений.

Система безопасности (СБ) - совокупность программных и аппаратных средств, предназначенных для мониторинга, записи, контроля и управления ресурсами обеспечения безопасности РостГМУ.

Администратор безопасности - должностное лицо, в обязанности которого входит выполнение функций по защите информации обрабатываемой, передаваемой и хранимой ИСПДн РостГМУ.

Системный администратор - должностное лицо, в обязанности которого входит системный контроль аппаратно-программных комплексов РостГМУ, управление доступом к информационным ресурсам и серверам, а также поддержание отказоустойчивости и безопасности данных, их резервное копирование и восстановление.

Пользователь – обучающийся, сотрудник РостГМУ, сотрудник подрядной организации и пациент клиники, использующий ресурсы информационных систем РостГМУ для обучения, выполнения должностных обязанностей и получения медицинских услуг.

Учетная запись - информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.). Учетные записи могут быть локальными и сетевыми (доменными).

Пароль - секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Изменение полномочий - процесс создания, удаления, внесения изменений в учетные записи пользователей ИС, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю ИС.

1. Общие положения

1.1. Настоящее Положение является локальным нормативным актом Федерального государственного бюджетного образовательного учреждения высшего образования «Ростовский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее по тексту РостГМУ), устанавливающим общие положения по обеспечению информационной безопасности РостГМУ.

1.2. Положение об информационной безопасности РостГМУ разработано в соответствии с действующим законодательством Российской Федерации, правовыми актами Министерства здравоохранения Российской Федерации, Уставом РостГМУ.

1.3. Информационная безопасность – это регламент действий пользователей в информационных сетях РостГМУ, направленный на обеспечение защиты информационных ресурсов РостГМУ от внешних и внутренних атак нарушителями.

1.4. Общее руководство и контроль за исполнением информационной безопасности возлагаются на проректора по безопасности и начальника департамента комплексной безопасности РостГМУ. Организация и практическое осуществление контроля соблюдения информационной безопасности возлагается на сотрудников отдела технической защиты (далее по тексту ОТЗ), сектор информационной безопасности (далее по тексту СИБ) ОТЗ департамента комплексной безопасности (далее по тексту СИБ ОТЗ ДКБ), а также на руководителей структурных подразделений РостГМУ.

1.5. Информационная безопасность предусматривает:

- учет информационных систем;
- создание и учет аккаунтов пользователей;
- создание и учет администраторов информационных систем и сетей;
- разработку структуры и схем защиты от внешних и внутренних атак нарушителями;
- анализ и аудит действий пользователей в информационных системах РостГМУ;
- контроль действий пользователей в интернет сети;
- контроль действий администраторов и пользователей при наполнении официальных сайтов РостГМУ.

1.6. Установленный настоящим Положением регламент информационной безопасности обязателен для всех сотрудников, обучающихся и сотрудников подрядных организаций РостГМУ.

1.7. Руководители структурных подразделений РостГМУ в обязательном порядке знакомят всеми доступными способами обучающихся и сотрудников РостГМУ с настоящим Положением и несут персональную ответственность за выполнение ими его требований.

1.8. В целях реализации настоящего Положения, разрабатываются регламенты. Все регламенты, указанные в данном Положении, подписываются проректором по безопасности РостГМУ и утверждаются приказом ректора РостГМУ.

1.9. Регламенты могут быть изменены на основании изменений в законодательстве Российской Федерации, административных и технических схем защиты информации.

Все изменения вносимые в регламенты публикуются на официальном сайте РостГМУ https://rostgmu.ru/ в разделе безопасность.

2. Организация системы обеспечения информационной безопасности

2.1. Система обеспечения информационной безопасности РостГМУ предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной защищенности в РостГМУ.

2.2. Для успешного функционирования системы обеспечения ИБ РостГМУ реализованы следующие процессы:

а) определение и уточнение области действия системы обеспечения ИБ и выбор подхода к оценке рисков ИБ (определение и уточнение области действия системы обеспечения ИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью РостГМУ, а также оценки правовых рисков деятельности РостГМУ);

б) анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов;

в) выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;

г) реализация системы обеспечения ИБ.

2.3. В целях реализации информационной безопасности РостГМУ устанавливается:

- защита персональных данных сотрудников, обучающихся и пациентов в соответствии с действующим законодательство Российской Федерации;
- контроль за использованием электронных средств информационного обеспечения деятельности РостГМУ по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности РостГМУ нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- внутрисетевой контроль за перемещением информации;
- запрет доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- проверка целесообразности использования сотрудниками и обучающимися РостГМУ интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- обучение персонала РостГМУ по вопросам обеспечения информационной безопасности.

3. Защита информационных ресурсов

3.1. Положением устанавливаются следующие категории информационных ресурсов:

3.1.1. **Открытая информация:**

- информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят;
- информация, сформированная в результате деятельности РостГМУ, которую запрещено относить к конфиденциальной на основании законодательства Российской Федерации;
- информация, представляемая в публичный доступ, используемая в деятельности РостГМУ.

3.1.2. **Информация ограниченного доступа:**

- информация, не содержащая сведений, составляющих государственную тайну (конфиденциальная информация) – это информация, доступ к которой ограничен федеральными законами.

3.2. В качестве основной угрозы безопасности конфиденциальной информации, включая персональные данные, рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

3.3. Защита информации в РостГМУ осуществляется путем исключения неправомерных или неосторожных действий со сведениями, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов РостГМУ.

3.4. Положение регламентирует:

а) порядок работы с документами, образцами, изделиями и другими источниками данных и информации;

б) круг лиц, которым разрешен доступ к использованию данных и информационных систем РостГМУ;

в) меры по контролю обращения с документами на любых носителях, содержащими конфиденциальные данные.

3.5. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых РостГМУ с данными лицами и организациями.

4. Учетные записи

4.1. Виды учетных записей:

- **Пользовательские** - предназначенные для идентификации и аутентификации пользователей информационных ресурсов РостГМУ;
- **Системные** - используемые операционной системой;
- **Служебные** - предназначенные для обеспечения функционирования отдельных процессов или приложений.

4.2. Порядок создания, изменения и удаление учетных записей:

4.2.1. Создание учетной записи пользователя для входа в операционную систему АРМ и доступа к сетевым ресурсам, производится администратором безопасности на основании его заявления (Приложение № 1) на имя начальника департамента комплексной безопасности, согласованное с руководителем структурного подразделения.

4.2.2. Заявления с отметками об исполнении и подписью заявителя хранятся в ОТЗ три года.

4.2.3. Внесение изменений в учетную запись или её удаление производится администратором безопасности на основании служебной записки (Приложение № 2) руководителя структурного подразделения на имя начальника департамента комплексной.

4.2.4. Ответственное лицо за ведение реестра учетных записей назначается и освобождается приказом Ректора из числа сотрудников СИБ ОТЗ ДКБ.

4.2.5. Ответственное лицо ведет реестр учетных записей на основании заявлений и служебных записок, переданных для регистрации в специальной электронной базе и журнале «Регистрации учетных записей» (Приложение № 3).

4.2.6. Создание, изменение и удаление учетной записи в информационных системах РостГМУ возлагается на ответственное лицо структурного подразделения, назначенное приказом ректора, которое осуществляет техническое обслуживание данной информационной системы. Учетные документы на пользователя формируются в соответствии с требованиями и регламентом информационной системы.

4.3. Ограничения, устанавливаемые на учетные записи:

4.3.1. При задании первичного пароля пользовательской учетной записи пользователя администратор безопасности и/или системный администратор обязан установить отметку «Потребовать смену пароля при первом входе в систему» при наличии технических возможности. Допускается в качестве первичного пароля использовать простые или повторяющиеся комбинации.

4.3.2. Служебные учетные записи - учетные записи, содержащие реквизиты, необходимые для нормального функционирования некоторых служб и сервисов (например, задачи резервного копирования и восстановления, служба автоматического обновления ОС и т.п.). Служебные учетные записи не предназначены для локального входа в систему, работа сотрудников с использованием реквизитов служебных учетных записей **Запрещена.**

4.3.3. Категорически **ЗАПРЕЩАЕТСЯ** всем пользователям использование встроенной учетной записей для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только системным администраторам, если технические работы требуют реквизитов именно этой учетной записи (восстановление системы, восстановление поврежденных данных системы, в некоторых случаях проведение обновлений системы и т.п.).

4.3.4. Решение о необходимости применения встроенных и служебных учетных записей принимает администратор безопасности и/или системный администратор.

4.4. Встроенные учетные записи:

4.4.1. Встроенные учетные записи компьютеров предназначены для служебного использования администратором безопасности и/или системным администратором при настройке системы и не предназначены для повседневной работы.

4.4.2. Создание и использование встроенных учетных записей на АРМ-ах, подключенных к информационным сетям РостГМУ **Запрещено**.

4.4.3. Встроенные учетные записи блокируется на всех АРМ-ах в составе ИС РостГМУ при первоначальном конфигурировании операционной системы.

4.5. Учетные записи администраторов:

4.5.1. Учетная запись администратора безопасности – предназначена для управления доступом на АРМ-ах, сетевых ресурсах и пограничных устройствах.

4.5.2. Учетная запись системного администратора – предназначена для управления доступом в информационных системах и на серверах.

5. Требования к паролям

5.1. Пользовательский пароль:

5.1.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливается администратором безопасности и/или системным администратором при создании новой учетной записи.

5.1.2. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

5.1.3. При создании первичного пароля, администратор безопасности и/или системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему *при технической возможности*, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

5.1.4. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику РостГМУ, используемая для подтверждения подлинности владельца учетной записи.

5.1.5. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

5.1.6. При выборе пароля необходимо руководствоваться следующими правилами:
- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов; - запрещается использовать в качестве пароля название учетной записи, фамилию пли имя пользователя, а также легко угадываемые сочетания символов.

5.1.7. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам управления информационных технологий (далее по тексту УИТ), записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.1.8. Пользователь обязан не реже одного раза в шесть месяцев производить смену основного пароля, соблюдая требования настоящего Положения.

5.1.9. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в ОТЗ и изменить основной пароль.

5.1.10. Восстановление забытого основного пароля пользователя осуществляется администратор безопасности путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменного объяснения (Приложение № 4) пользователя на имя начальника департамента комплексной безопасности, после исполнения объяснительная передается для внесения изменений в реестр пользователей.

5.1.11. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5.1.12. Разблокирование учетной записи пользователя осуществляется администратор безопасности на основании письменного объяснения (Приложение № 4) пользователя на имя

начальника департамента комплексной безопасности после исполнения объяснительная передается для внесения изменений в реестр пользователей.

5.2. Административный пароль:

5.2.1. Административный пароль – сложная комбинация символов (буквы, цифры, символы), используемая при настройке операционных и информационных систем, служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

5.2.2. Административный пароль на АРМ-ы и пограничные устройства, устанавливается администратор безопасности РостГМУ.

5.2.3. Административный пароль на сервера и информационные системы РостГМУ, устанавливается системным администратором.

5.2.4. Администратор безопасности и системный администратор несет персональную ответственность за сохранение в тайне пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.2.5. Администратор безопасности и системный администратор обязан не реже одного раза в три месяца производить смену пароля, соблюдая требования настоящего Положения.

5.2.6. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в ОТЗ и изменить пароль.

5.2.7. Смена забытого пароля системного администратора осуществляется начальником управления информационных технологий путем изменения (сброса) основного пароля на первичный пароль на основании письменного объяснения (Приложение № 5) системного администратора на имя проректора по безопасности, после исполнения объяснительная передается в департамент комплексной безопасности.

5.2.8. Смена забытого пароля администратора безопасности осуществляется руководителем ОТЗ путем изменения (сброса) основного пароля на первичный пароль на основании письменного объяснения (Приложение № 5) администратора безопасности на имя проректора по безопасности, после исполнения объяснительная передается в департамент комплексной безопасности.

6. Электронные подписи

6.1. Создание, получение, хранение и использование ЭП сотрудниками РостГМУ определяются «Регламентом об электронных подписях».

6.2. Первичное получение ЭП и настройка программного обеспечения осуществляется сотрудниками СИБ ОТЗ ДКБ.

6.3. Техническая помощь пользователям в получении ЭП и ведение учёта ЭП возложено на сотрудников СИБ ОТЗ ДКБ.

6.4. **Отслеживание срока окончания ЭП, продление ЭП полностью возлагается на владельца ЭП.**

6.5. Восстановление ЭП, при истечении срока действия и (или) утери пароля, контейнера ЭП, нарушении сроков получения ЭП у аккредитованных центров и других ошибках пользователя проводится сотрудниками СИБ ОТЗ ДКБ исключительно по письменному обращению владельца ЭП на имя проректора по безопасности;

6.6. Установка программного обеспечения, настройка АРМ-ов и техническое сопровождение пользователей для работы с ЭП возложено на сотрудников УИТ.

7. Установка нового оборудования, подключение к сети РостГМУ

7.1. Установка и обслуживание оборудования, подключение к локальной сети РостГМУ производится исключительно сотрудниками УИТ, а также при выполнении специальных работ сотрудниками ОТЗ и представителями сертифицированных интеграторов в рамках договорных работ.

7.2. Подключение стороннего оборудования: WiFi роутеров, ноутбуков и других технических средств, представляющих угрозу информационной безопасности РостГМУ **КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО**:

7.2.1. На работников УИТ возлагается обязанность по отключению и изыманию данных устройств у структурных подразделений РостГМУ.

7.2.2. Сотрудниками ОТЗ департамента комплексной безопасности проводится служебная проверка в отношении нарушителей данного Положения.

7.3. Для определения несанкционированной замены оборудования новые и попадающие на обслуживание в УИТ АРМ-ы РостГМУ должно быть опечатаны в местах возможного вскрытия.

7.4. Техническое обслуживание оборудования ЛВС и информационных систем РостГМУ возлагается на сотрудников УИТ. Все регламентные и ремонтные работы регистрируются в журнале «Обслуживания оборудования и программного обеспечения» в электронном виде.

7.5. Ответственность за сбои в работе серверного оборудования возлагается на сотрудников УИТ.

8. Установка программного обеспечения, перечень основных программ рабочего места пользователя

8.1 Установка и обслуживание программного обеспечения его настройка производится исключительно сотрудниками УИТ, а также при выполнении специальных работ сотрудниками ОТЗ и представителями сертифицированных интеграторов в рамках договорных работ. Установка и обслуживание программного обеспечения его настройка сотрудниками других структурных подразделений **Запрещена**.

8.2. Ответственность за сбои в работе информационных систем РостГМУ возлагается на сотрудников УИТ.

9. Архивирование и хранение, копирование информации

9.1. Служебная информация сотрудников РостГМУ должна храниться на АРМах сотрудников и на серверах РостГМУ.

9.2. Для обеспечения целостности данных необходимо проводить резервное копирование критически важных БД не реже одного раза в сутки. Ответственность за резервное копирование БД РостГМУ возлагается на сотрудников УИТ.

9.3 **Запрещено** копирование и хранение служебной информации на личных носителях информации сотрудников.

10. Правила доступа к ресурсам интернет и работы с электронной почтой

10.1 Доступ в Интернет для сотрудников предоставляется для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам деятельности.

10.2. Доступ к ресурсам Интернет может быть блокирован администратором безопасности или системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных законодательством Российской Федерации и внутренними регламентными документами.

10.3. Правила работы с ресурсами Интернет указаны в Приложении № 6.

10.4. Для исполнения задач, связанных с служебной деятельностью сотрудников РостГМУ может быть предоставлен доступ к системе электронной почты. Использование системы электронной почты РостГМУ в других целях **Запрещено**.

Вся служебная переписка должна вестись строго с использованием этого электронного адреса.

10.5. Доступ к системе электронной почты предоставляется сотруднику РостГМУ одновременно с предоставлением учетной записи пользователя.

10.6. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию руководства университета.

10.7. Пользуясь электронной почтой и ресурсами Интернета с рабочего места, сотрудник обязан соблюдать принципы делового общения и этикета.

10.8. Запрещается передавать по электронной почте конфиденциальную информацию в незашифрованном виде, переходить по подозрительным ссылкам.

10.9. Доступ к электронной почте может быть блокирован администратором безопасности или системным администратором без предварительного уведомления при возникновении нештатных ситуаций, либо в иных случаях, предусмотренных внутренними документами.

10.10. Правила работы с электронной почтой указаны в Приложении № 7.

11. Антивирусная защита

11.1. Основным способом защиты информации от воздействия компьютерных вирусов на АРМ является применение средств антивирусной защиты (далее — САВЗ). К использованию в РостГМУ допускаются только лицензионные антивирусные средства, сертифицированные и допущенные к применению в Российской Федерации, имеющие сервер централизованного администрирования и программы-агенты для установки на сервера и персональные компьютеры, обеспечивающие централизованный мониторинг и управление антивирусом. Антивирусному контролю подлежит любая информация, поступающая на персональные компьютеры Пользователей, в том числе из сети Интернет и с внешних носителей.

11.2. Обновление антивирусных баз на АРМ-ах и серверах РостГМУ производится автоматически с серверов обновления разработчика антивируса или с сервера антивирусной защиты.

11.3. В случае обнаружения зараженных компьютерными вирусами файлов пользователь **ОБЯЗАН**:

- приостановить работу;
- поставить в известность о факте обнаружения зараженных вирусом файлов УИТ и ОТЗ.

11.4. Установка средств антивирусного контроля на компьютерах (серверах ЛВС) РостГМУ возлагается исключительно на сотрудников УИТ и ОТЗ.

11.5. Настройка параметров средств антивирусного контроля осуществляется сотрудниками УИТ в соответствии с принятой политикой информационной безопасности РостГМУ. От изменения настроек Пользователем, антивирусное программное обеспечение должно быть защищено паролем.

11.6. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов оборудования.

11.7. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

11.8. **Полная антивирусная проверка в ручном режиме должна проводиться Пользователем не реже одного раза в месяц.**

11.9. Полная антивирусная проверка на серверах ЛВС в автоматическом режиме должна производиться не реже одного раза в неделю. Ответственность за проведение данного регламента возлагается на системных администраторов ЛВС РостГМУ.

12. Закрытая сеть систем безопасности РостГМУ

12.1. Для обеспечения управления контролем доступа, сбором видеоинформации, а также для ведения специального учета в РостГМУ создана закрытая локальная сеть для функционирования систем безопасности университета.

12.2. Установка и обслуживание оборудования, подключение к закрытой сети систем безопасности РостГМУ производится исключительно сотрудниками ОТЗ.

12.3 Установка и обслуживание программного обеспечения его настройка на закрытой сети систем безопасности производится исключительно сотрудниками ОТЗ

12.4. Регламентное обслуживание оборудования и программного обеспечения закрытой сети систем безопасности РостГМУ возлагается на сотрудников ОТЗ. Все регламентные работы регистрируются в журнале «Плановых и ремонтных работ» (Приложение № 8).

12.5. Администрирование закрытой сети систем безопасности РостГМУ возлагается на руководителя ОТЗ.

12.6. Создание, изменение и удаление учетных записей в закрытой сети систем безопасности РостГМУ возлагается исключительно на руководителя ОТЗ. Реестр пользователей закрытой сети систем безопасности РостГМУ ведется руководителем ОТЗ в электронном виде.

12.7. Предоставление доступа к закрытой сети систем безопасности РостГМУ пользователей ЛВС РостГМУ производится на основании служебной записки на имя ректора РостГМУ от руководителя структурного подразделения с обязательным согласованием проректора по направлению.

12.8. Предоставление информации или копирование данных из БД систем безопасности производится исключительно по письменному запросу правоохранительных органов и (или) служебной записке на имя ректора РостГМУ от руководителя структурного подразделения с обязательным согласованием проректора по направлению.

13. Ответственность за нарушение Положения

13.1. Ответственность за выполнение требований настоящего Положения РостГМУ, сотрудниками, посетителями, пациентами, обучающимися, сотрудниками подрядных организаций, возлагается на руководителей структурных подразделений РостГМУ.

13.2. За нарушение требований настоящего Положения сотрудники, посетители, пациенты, обучающиеся, сотрудники – подрядных организации, несут материальную, дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

13.2. В случае если действия сотрудников, посетителей, пациентов, обучающихся, сотрудников подрядных организаций, нарушающих требования настоящего Положения, содержат состав административного правонарушения, уголовного преступления, информация о данном факте подлежит передаче в территориальный отдел полиции ГУ МВД России по Ростовской области.

Согласовано:

Проректор по безопасности В.Н. Кандыба

«___» _____2024 г.

Начальник правового управления А.В. Макарова

«___» _____2024 г.

Начальник управления

информационных технологий В.А. Руденко

«___» _____2024 г.

Приложение № 1
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

Начальнику департамента комплексной безопасности
ФГБОУ ВО РостГМУ Минздрава России

ЗАЯВЛЕНИЕ

на создание учетной записи пользователя

Логин (заполняется администратором безопасности)	
Уровень прав пользователя (заполняется администратором безопасности)	
Электронная почта (заполняется администратором безопасности)	
Ф.И.О. (полностью)	
Подразделение	
Должность	
Телефон	

_____ ( ) «____»_____20___ г.

(подпись сотрудника) Ф.И.О.

Руководитель подразделения _____ ( )

Согласовано, начальник

департамента комплексной безопасности: _____ ( )

Департамент комплексной безопасности

Отметка о регистрации пользователя	**Первоначальный пароль получил**
«___»_____20___г._____	

Отметка о внесении в реестр пользователя	**Учетная запись удалена**
«___»_____20___г._____	«___»_____20___г._____

Лист ознакомления

Выписка из «Положения об информационной безопасности»

Термины и определения

ЛВС – локальная вычислительная сеть.
УИТ – управление информационных технологий.
ОТЗ – отдел технической защиты департамента комплексной безопасности.

4.2. Порядок создания, изменения и удаление учетных записей:

4.2.1. Создание учетной записи пользователя для входа в операционную систему рабочей станции и доступа к сетевым ресурсам, производится администратором безопасности на основании его заявления (Приложение № 1) на имя начальника департамента комплексной безопасности, согласованное с руководителем структурного подразделения.

4.2.3. Внесение изменений в учетную запись или её удаление производится администратором безопасности на основании служебной записки (Приложение № 2) руководителя структурного подразделения на имя начальника департамента комплексной безопасности.

5.1. Пользовательский пароль:

5.1.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливается администратором безопасности и/или системным администратором при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности и/или системном администраторе).

5.1.3. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

5.1.5. Первичный пароль также используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

5.1.6. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику РостГМУ, используемая для подтверждения подлинности владельца учетной записи.

5.1.7. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

5.1.8. При выборе пароля необходимо руководствоваться следующими правилами:
- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов; - запрещается использовать в качестве пароля название учетной записи, фамилию пли имя пользователя, а также легко угадываемые сочетания символов.

5.1.9. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам УИТ, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.1.10. Пользователь обязан не реже одного раза в шесть месяцев производить смену основного пароля, соблюдая требования настоящего Положения.

5.1.11. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в ОТЗ и изменить основной пароль.

5.1.12. Восстановление забытого основного пароля пользователя осуществляется администратор безопасности путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменного объяснения (Приложение № 4) пользователя на имя начальника департамента комплексной безопасности, после исполнения объяснительная передается для внесения изменений в реестр пользователей.

5.1.13. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5.1.14. Разблокирование учетной записи пользователя осуществляется администратор безопасности на основании письменного объяснения (Приложение № 4) пользователя на имя начальника департамента комплексной безопасности после исполнения объяснительная передается для внесения изменений в реестр пользователей.

9. Правила доступа к ресурсам интернет и работы с электронной почтой

9.1 Доступ в Интернет для сотрудников предоставляется для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам деятельности.

9.5. Доступ к системе электронной почты предоставляется сотруднику РостГМУ одновременно с предоставлением учетной записи пользователя.

9.11 Пользуясь электронной почтой и ресурсами Интернета с рабочего места, сотрудник обязан соблюдать принципы делового общения и этикета.

9.12 Запрещается передавать по электронной почте конфиденциальную информацию в незашифрованном виде, переходить по подозрительным ссылкам.

10. Антивирусная защита

10.3. В случае обнаружения зараженных компьютерными вирусами файлов пользователь **ОБЯЗАН**:
- приостановить работу;
- поставить в известность о факте обнаружения зараженных вирусом файлов УИТ и ОТЗ.

10.8. Полная антивирусная проверка в ручном режиме должна проводиться Пользователем не реже одного раза в месяц.

С правилами ознакомлен лично, второй экз. получил _____ ( )

«____» _____20___г.

Приложение № 2
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»

СЛУЖЕБНАЯ ЗАПИСКА

_____ № _____

Начальнику департамента
комплексной безопасности
ФГБОУ ВО РостГМУ
Минздрава России
Габуния А.Ю.

_____

(Ф.И.О. руководителя подразделения)

_____

(наименование подразделения)

В связи с _____,
(с переводом, изменением обязанностей и т.д.)

прошу изменить уровень доступа к рабочей станции и/или сетевому ресурсу РостГМУ_____,

(Ф.И.О. полностью)

_____ с «___»_____20__г.

(должность)

_____

(указать необходимый функционал)

Руководитель подразделения _____ ( )

Согласовано, начальник

департамента комплексной безопасности: _____ ( )

Департамент комплексной безопасности

Логин (заполняется администратором безопасности)		
Уровень прав пользователя (заполняется администратором безопасности)	Вносимые изменения в права пользователя	
	Текущий уровень	После изменения

Отметка о внесении изменений
«___»_____20___г._____

Отметка о внесении изменений в реестр
«___»_____20___г._____

Приложение № 3
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

ФГБОУ ВО РОСТГМУ
Минздрава России
ДЕПАРТАМЕНТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

ЖУРНАЛ

Регистрации учетных записей

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
Итого внесено _____ записей.

Срок хранения три года

Логин	Дата регистрации	Ф.И.О. пользователя (полностью	Уровень прав пользователя	Роспись пользователя	Роспись администратора безопасности
1	2	3	4		

Приложение № 4
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

Начальнику департамента комплексной безопасности
ФГБОУ ВО РостГМУ Минздрава России
Габуния А.Ю.

_____

(Ф.И.О. пользователя)

_____

(наименование подразделения)

О Б Ъ Я С Н И Т Е Л Ь Н А Я

_____

_____

_____

_____

_____

Дата заполнения «____»_____20__ г. Подпись _____

Департамент комплексной безопасности

Отметка о внесении изменений
«___»_____20___г._____ _____

Отметка о внесении изменений в реестр
«___»_____20___г._____

Лист ознакомления

Выписка из «Положения об информационной безопасности»

Термины и определения

УИТ – управление информационных технологий.

ОТЗ – отдел технической защиты департамента комплексной безопасности.

5.1. Пользовательский пароль:

5.1.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливается администратором безопасности и/или системным администратором при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности и/или системном администраторе).

5.1.2. Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

5.1.3. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

5.1.5. Первичный пароль также используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

5.1.6. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику РостГМУ, используемая для подтверждения подлинности владельца учетной записи.

5.1.7. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

5.1.8. При выборе пароля необходимо руководствоваться следующими правилами:

- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов; - запрещается использовать в качестве пароля название учетной записи, фамилию пли имя пользователя, а также легко угадываемые сочетания символов.

5.1.9. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам УИТ, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.1.10. Пользователь обязан не реже одного раза в шесть месяцев производить смену основного пароля, соблюдая требования настоящего Положения.

5.1.11. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в ОТЗ и изменить основной пароль.

5.1.12. Восстановление забытого основного пароля пользователя осуществляется администратор безопасности путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменного объяснения (Приложение № 4) пользователя на имя начальника управления безопасности, после исполнения объяснительная передается для внесения изменений в реестр пользователей.

5.1.13. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5.1.14. Разблокирование учетной записи пользователя осуществляется администратор безопасности на основании письменного объяснения (Приложение № 4) пользователя на имя начальника управления безопасности после исполнения объяснительная передается для внесения изменений в реестр пользователей.

С «Положением об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России», а также регламентами к нему ознакомлен:

_____(_____) «____»_____20__г.

Приложение № 5
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

Проректору по безопасности
ФГБОУ ВО РостГМУ Минздрава России
Кандыба В.Н.

_____

(Ф.И.О. пользователя)

_____

(наименование подразделения)

О Б Ъ Я С Н И Т Е Л Ь Н А Я

_____

_____

_____

_____

_____

Дата заполнения «____»_____20__ г. Подпись _____

Департамент комплексной безопасности

Отметка о внесении изменений
«___»_____20___г._____ _____

Отметка о внесении изменений в реестр
«___»_____20___г._____

Лист ознакомления

Выписка из «Положения об информационной безопасности»

Термины и определения

УИТ – управление информационных технологий.

ОТЗ – отдел технической защиты департамента комплексной безопасности.

5.2. Административный пароль:

5.2.1. Административный пароль – сложная комбинация символов (буквы, цифры, символы), используемая при настройке операционных и информационных систем, служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

5.2.2. Административный пароль на АРМ-ы и пограничные устройства, устанавливается администратор безопасности РостГМУ.

5.2.3. Административный пароль на сервера и информационные системы РостГМУ, устанавливается системным администратором.

5.2.4. Администратор безопасности и системный администратор несет персональную ответственность за сохранение в тайне пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.2.5. Администратор безопасности и системный администратор обязан не реже одного раза в три месяца производить смену пароля, соблюдая требования настоящего Положения.

5.2.6. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в ОТЗ и изменить пароль.

5.2.7. Смена забытого пароля системного администратора осуществляется начальником управления информационных технологий путем изменения (сброса) основного пароля на первичный пароль на основании письменного объяснения (Приложение № 5) системного администратора на имя проректора по безопасности, после исполнения объяснительная передается в департамент комплексной безопасности.

5.2.8. Смена забытого пароля администратора безопасности осуществляется руководителем ОТЗ путем изменения (сброса) основного пароля на первичный пароль на основании письменного объяснения (Приложение № 5) администратора безопасности на имя проректора по безопасности, после исполнения объяснительная передается в департамент комплексной безопасности.

С «Положением об информационной безопасности ФГБОУ ВО РостГМУ Минздрава России», а также регламентами к нему ознакомлен:

_____(_____) «____»_____20__г.

Приложение № 6
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

ПРАВИЛА
работы с ресурсами сети Интернет

1.1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. УИТ и департамент комплексной безопасности имеет право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие экстремистскую, вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

1.2. При работе с ресурсами сети Интернет недопустимо:

1.2.1. разглашение информации для служебного пользования, ставшей известной сотруднику РостГМУ по служебной необходимости либо иным путем;

1.2.2. распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

1.2.3. публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

1.3. При работе с ресурсами Интернет запрещается:

1.3.1. загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

1.3.2. использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой РостГМУ.

1.4. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой РостГМУ.

1.5. Вся информация о ресурсах, посещаемых сотрудниками РостГМУ, контролируется и, при необходимости, может быть предоставлена администрации университета, а также руководителям структурных подразделений для детального изучения.

Приложение № 7
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

ПРАВИЛА
работы с электронной почтой

1. Электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически **Запрещено**.

2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

3. При работе с системой электронной почты РостГМУ сотрудникам запрещается:

3.1. использовать адрес почты РостГМУ для оформления подписок и массовых рассылок;

3.2. публиковать свой адрес, либо адреса других сотрудников РостГМУ на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

3.3. отправлять сообщения с вложенными файлами общий объем которых превышает 20 Мегабайт, без согласования с департаментом комплексной безопасности;

3.4. открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

3.5. осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;

3.6. осуществлять массовую рассылку почтовых сообщений рекламного характера;

3.7. рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

3.8. распространять защищаемые авторскими правами материалы, затрагивающие какой- либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей сторон;

3.9. распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие экстремистскую, вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д. распространять информацию ограниченного доступа, представляющую коммерческую тайну;

3.10. предоставлять кому бы то ни было пароль для доступа к своему почтовому адресу.

Приложение № 8
к Положению об информационной безопасности
ФГБОУ ВО РостГМУ Минздрава России

ФГБОУ ВО РОСТГМУ
Минздрава России
ДЕПАРТАМЕНТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

ЖУРНАЛ

Плановых и ремонтных работ ОТЗ

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
Срок хранения три года

Дата	Время начала работ	Место проведения работ	Краткий перечень выполненных работ	Время окончания работ	Роспись сотрудника
1	2	3	4	5	6