ПРИНЯТО
ученым советом ФГАОУ ВО РНИМУ
им. Н.И. Пирогова Минздрава России
(Пироговский Университет)
Протокол № 4
от 15.12.2025

УТВЕРЖДЕНО
приказом ФГАОУ ВО РНИМУ
им. Н.И. Пирогова Минздрава России
(Пироговский Университет)
№ 2235 рук
от 18.12.2025

ПОЛИТИКА
ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет) в области информационной безопасности

г. Москва

2025

Оглавление

1. Вводные положения

Назначение

Политика Университета является основополагающим документом, предназначенным для выражения позиции ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России (Пироговский Университет) в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности образовательных, научных, исследовательских, медицинских, финансово-хозяйственных и иных процессов Университета, направленных на достижение целей, предусмотренных Уставом Университета, создания условий безопасного цифрового развития Университета и обеспечения соответствия требованиям законодательства Российской Федерации в данной области.

Политика Университета разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

Область действия

Политика Университета обязательна для исполнения работниками федерального государственного автономного образовательного учреждения высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации.

Политика Университета не распространяется на организацию и порядок защиты информации, составляющей государственную тайну.

Период действия и порядок внесения изменений

Политика Университета является локальным нормативным документом постоянного действия.

Политика Университета утверждается, изменяется и признается утратившей силу в Университете в соответствии с приказом Университета.

2. Основные термины и сокращения

В настоящем Регламенте применяются следующие основные термины и сокращения:

Университет	Федеральное государственное автономное образовательное учреждение высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации и его обособленные структурные подразделения, филиалы.
Деловой партнер	Текущие и потенциальные контрагенты Университета.
Информация	Сведения (сообщения, данные) независимо от формы их представления.
Информационный актив	Информационные ресурсы и средства обработки информации (информационные, технические, программные), в информационных системах и сетях Университета.
Информационно-технологическая инфраструктура	Комплексная структура, объединяющая все информационные технологии и ресурсы, используемые Университетом. Информационно - технологическая инфраструктура включает все компьютеры, установленное программное обеспечение, системы связи, информационные центры, сети и базы данных.
ИТ-актив	Идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Университета.
ИТ-пространство	Совокупность объектов (информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура), вступающих друг с другом в информационное взаимодействие, а также сами

	информационные технологии, обеспечивающие данное взаимодействие.
Абитуриент	Физическое лицо, подающее документы для поступления в Университет. Статус абитуриента прекращается с момента зачисления в Университет.
Обучающийся	Физическое лицо, осваивающее образовательную программу. В зависимости от уровня осваиваемой образовательной программы, формы обучения и режима пребывания в Университете к обучающимся относятся: слушатели, студенты, бакалавры, магистры, экстерны, ординаторы, аспиранты, ассистенты-стажеры.
Пациент	Физическое лицо, которому оказывается медицинская помощь (медицинские услуги) или которое обратилось за оказанием медицинской помощи (медицинских услуг) в структурные подразделения Университета, независимо от наличия у него заболевания и от его состояния.
Процессы Университета	Образовательные, научные, исследовательские, медицинские, финансово-хозяйственные и иные процессы Университета, направленные на достижение целей, предусмотренных Уставом Университета.
Риск информационной безопасности (ИБ-риск)	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива.
Средства защиты информации	Специализированные программные, программно-аппаратные средства, предназначенные для решения задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Цифровизация	Применение прорывных технологий, трансформирующих операционные процессы за счет замещения или дополнения человека на базе использования качественно новой аналитики, искусственного интеллекта, мобильных и носимых устройств, роботизации, интеграционных технологических платформ.

3. Заявление о политике в области информационной безопасности

Политика Университета выражает позицию Университета в области информационной безопасности. Принятием ее Университет провозглашает и обязуется осуществлять все возможные меры для защиты работников, абитуриентов, обучающихся, пациентов и контрагентов, а также имущества, информации, деловой репутации и Процессов Университета от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Университета осознает важность и необходимость продвижения и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства Российской Федерации и регулирования норм информационной безопасности, а также развития используемых информационных технологий при автоматизации и цифровизации в Университете. Соблюдение принципов информационной безопасности дополнительно позволит упрочить конкурентные преимущества Университета, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить имиджевые риски.

Политика Университета разработана с целью установления принципов, определяющих общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Университета и защиты интересов Университета от рисков и угроз информационной безопасности.

Руководство Университета придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является безусловным и необходимым элементом в работе Университета. Следование требованиям информационной безопасности является важным условием при

осуществлении повседневной деятельности (в том числе при реализации ИТ-проектов, проработке цифровых инициатив и т.д.), включая образовательную, научную, медицинскую и фармацевтическую деятельности, а также совместную работу с Деловыми партнерами Университета. Каждый работник Университета и его Деловые партнеры несут ответственность за безопасную работу с вверенными им информационными активами, компьютерным оборудованием, виртуальной инфраструктурой, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Университета.

Руководители и специалисты по информационной безопасности Университета должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищённости информации, информационных активов, информационно-технологической инфраструктуры и Процессов Университета.

Работники Университета должны руководствоваться Политикой Университета в профессиональной деятельности, взаимодействии, личном развитии и повышении культуры информационной безопасности.

4. Цели и задачи Университета в области информационной безопасности

Управление и обеспечение информационной безопасности Университета ориентированы на достижение следующих целей в области информационной безопасности:

- предоставление безопасной информационной среды для функционирования и развития Процессов Университета;
- снижение уровня рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое цифровое развитие Университета.

Для достижения данных целей необходимо решение следующих задач:

- обеспечение информационной безопасности Процессов Университета в условиях возрастающего уровня угроз, включая обеспечение оперативного мониторинга и оценку состояния защищенности в Университете; повышение эффективности защиты от спланированных целенаправленных компьютерных атак

злоумышленниками; повышение информационной безопасности технологических и образовательных систем;

- применение новых современных методов для защищенной цифровизации Университета, включая организацию проработки вопросов информационной безопасности при реализации цифровых решений; организацию апробации и применения новых методов защиты информации от современных угроз, в том числе за счет взаимодействия и партнерства с лидерами отрасли информационной безопасности; обеспечение применения безопасных цифровых технологий при внедрении отечественных разработок и развитии собственного конкурентоспособного программного обеспечения Университета;
- соответствие требованиям государства в области информационной безопасности путем обеспечения заданного уровня информационной безопасности информационных активов в соответствии с требованиями действующего законодательства.

5. Объекты обеспечения информационной безопасности

В рамках обеспечения информационной безопасности объектами защиты в Университете является информация, обрабатываемая в Университете, вне зависимости от формы представления; информационные активы, включая, но не ограничиваясь следующим перечнем:

- автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
- информационные системы, системы хранения данных, программное обеспечение и отдельные технические решения;
- автоматизированные системы, в том числе медицинские и измерительные системы;
- информационно-технологическая и виртуальная инфраструктура;
- информационно - телекоммуникационные сети и системы связи;
- информационные сервисы (ИТ-услуги), оказываемые Университету или в интересах Университета;

- решения по цифровизации Процессов Университета.

6. Принципы управления и обеспечения информационной безопасности

Деятельность Университета в области информационной безопасности осуществляется с соблюдением следующих основных принципов[1]:

Ориентация на стратегию Университета – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития Университета, с учетом стратегий в области информационных технологий и технологий автоматизации.

Централизация функций управления – принцип заключается в возможности принятия управленческих решений в области информационной безопасности на уровне Университета за счет оперативного мониторинга (ИТ-пространства Университета и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности; осуществления централизованного управления стратегическими инициативами по информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности; создания и развития централизованных решений в области информационной безопасности.

Проактивный подход и управление рисками – базируется на мониторинге, анализе и оценке появляющихся, актуальных и будущих рисков и угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Университету.

Стандартизация и унификация – подразумевает разработку и тиражирование в филиалах и обособленных структурных подразделениях Университета стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения информационной безопасности для унификации средств, и методов решения однотипных задач, интерфейсов управления системами информационной безопасности.

[1] Разработаны с учетом межгосударственного стандарта ГОСТ ISO/IEC 27014-2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности»

Импортозамещение – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счёт ориентирования на отечественные решения, средства и сервисы при обеспечении информационной безопасности на территории Российской Федерации.

Ресурсное обеспечение – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной безопасности Университета, поддержание требуемой организационной структуры.

Законность и соответствие – деятельность по обеспечению информационной безопасности Университета основывается на выполнении требований нормативных правовых актов Российской Федерации.

Повышение культуры информационной безопасности – декларирует необходимость не только информировать всех работников Университета, абитуриентов, обучающихся, пациентов, его Деловых партнёров и других лиц, использующих ИТ-активы Университета, о требованиях информационной безопасности, но развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами Университета.

Развитие компетенций и профессионализма – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей. Обеспечение информационной безопасности при автоматизации Процессов Университета требует компетенций и знаний в областях производственной автоматизации.

Накопление знаний и обмен опытом – следует накапливать знания и обмениваться опытом в ходе осуществления практической деятельности по обеспечению информационной безопасности (при мониторинге и реагировании на компьютерные атаки, при внедрении и эксплуатации технических решений, при аудитах информационной безопасности и т.д.).

Информационная безопасность как неотъемлемое свойство ИТ-актива – принцип заключается в следующем:

- требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива, вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе;
- создание программных продуктов в интересах Университета осуществляется с применением методов безопасной разработки программного обеспечения;
- предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);
- встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;
- соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

Информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги) – означает, что предлагаемые и оказываемые Университету или в интересах Университета ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

Совместимость – подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость на информационном, программном, электромагнитном и эксплуатационном уровнях, а также совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации Процессов Университета.

Надежность – использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

Адекватность и обоснованность решений – принимаемые в Университете меры и применяемые средства информационной безопасности эффективны,

результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Университета.

Комплексность – применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба Университету, его Деловым партнёрам и работникам.

Разделение и минимизация полномочий – означает, что выполнение критичных (итоговых) операций проводится только посредством разделения действий (например, алгоритмического разделения, временного или ресурсного – в том числе двумя работниками). Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделений полномочий является предпочтительным относительно организационного. Должны осуществляться контроль реализации принципов разграничения критических полномочий в ИС и в АСУ, ограничение прав доступа, в зависимости от уровня согласованных полномочий. Полномочия должны быть минимально достаточными для выполнения лицом своих должностных обязанностей, либо выполнения контрактных обязательств. При необходимости должен осуществляться организационный и программно-аппаратный контроль конфликта полномочий.

Постоянство совершенствования информационной безопасности – обеспечение постоянного улучшения существующей практики и совершенствования средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области.

7. Ответственность за нарушения в области информационной безопасности

Работники Университета должны выполнять требования и правила информационной безопасности при работе с информацией, в том числе касающейся самих работников, абитуриентов, обучающихся, пациентов и Деловых партнёров, а также при работе с ИТ-активами Университета и Деловых партнёров.

Требования распорядительных документов и правил обеспечения информационной безопасности обязательны для всех без исключения работников Университета и должны учитываться во взаимоотношениях с абитуриентами, обучающимися, пациентами и Деловыми партнерами.

Руководство Университета возлагает ответственность на руководителей структурных подразделений, представительств и филиалов Университета за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей Процессов Университета; за своевременную идентификацию значимых ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Университета, абитуриентам, обучающимся, пациентам и Деловым партнерам, использующим ИТ-активы Университета, и контроль за их выполнением.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, сайтов, других средств телекоммуникаций и мобильных технических средств работникам Университета рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации.

Каждый работник Университета за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

Работники Деловых партнёров, абитуриенты, обучающиеся, пациенты, использующие ИТ-активы Университета, а также предоставленную Университетом информацию, несут ответственность в соответствии с договорными отношениями с Университетом, а также применимым законодательством.

8. Доведение и распространение Политики Университета

8.1. Политика Университета является публичной. Университет доводит Политику Университета до абитуриентов, обучающихся, пациентов и своих Деловых партнеров и взаимодействует с ними с учетом Политики Университета.

8.2. Настоящее положение принимается ученым советом федерального государственного автономного образовательного учреждения высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации и утверждается приказом федерального государственного автономного образовательного учреждения высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации.

8.3. Изменения и дополнения в настоящее Положение принимается и утверждается в том же порядке, в котором принято и утверждено настоящее Положение.