Межгосударственное образовательное учреждение высшего образования «Белорусско-Российский университет»

УТВЕРЖДЕНО
Приказ ректора Белорусско-Российского университета
от 21.10.2025 №544

ПОЛИТИКА
информационной безопасности Белорусско-Российского университета

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности межгосударственного образовательного учреждения высшего образования «Белорусско-Российский университет» (далее – Политика) определяет цели, задачи, принципы и основные направления деятельности Белорусско-Российского университета (далее – Университет) по обеспечению информационной безопасности (далее – ИБ) информационных систем (далее – ИС) в Университете.

2. Настоящая Политика представляет собой официально принятую в Университете систему взглядов на проблему обеспечения ИБ и является основополагающим документом для построения и функционирования системы защиты информации.

3. Нормативной правовой основой настоящей Политики являются:

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

иные нормативные правовые акты Республики Беларусь и Российской Федерации, локальные правовые акты Университета в области информатизации и защиты информации.

4. Действие настоящей Политики распространяется на все структурные подразделения, всех работников, обучающихся и иных лиц, имеющих доступ к информационным системам, сетям и ресурсам Университета.

5. Политика не затрагивает вопросы обеспечения безопасности информации, содержащей сведения, составляющие государственные секреты, защита которых регламентируется отдельными законодательными актами Республики Беларусь.

6. Положения настоящей Политики являются обязательными для исполнения всеми субъектами информационных отношений Университета и служат основой для разработки других локальных правовых актов, регламентирующих вопросы обеспечения информационной безопасности.

7. Настоящая Политика подлежит пересмотру и актуализации на регулярной основе, но не реже одного раза в два года, а также при возникновении существенных изменений в законодательстве Республики Беларусь, активов информационных систем или информационных процессах деятельности Университета.

ГЛАВА 2
ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

8. Основной целью защиты информации в Университете является защита его информационных активов от внутренних и внешних угроз для обеспечения конфиденциальности, целостности, доступности, подлинности и сохранности обрабатываемой информации, а также минимизация возможного ущерба от инцидентов информационной безопасности.

9. При обеспечении защиты информации подлежат решению основные задачи по обеспечению информационной безопасности:

реализация требований законодательства Республики Беларусь в части обеспечения информационной безопасности информационных систем и осуществление контроля за их защищенностью;

своевременное выявление, оценка и прогнозирование угроз информационной безопасности, а также причин и условий, способствующих нанесению ущерба субъектам информационных отношений и нарушению функционирования систем Университета;

создание условий для минимизации и предотвращения ущерба от неправомерных действий, а также ослабление негативного влияния и ликвидация последствий нарушений информационной безопасности;

обеспечение защиты от несанкционированного вмешательства в процесс функционирования информационных систем со стороны посторонних лиц;

чёткое разграничение доступа пользователей к информационным, аппаратным и программным ресурсам Университета, предоставление доступа только к тем ресурсам и операциям, которые необходимы для выполнения их должностных обязанностей;

обеспечение аутентификации пользователей, имеющих допуск в информационные системы и участвующих в информационном обмене;

защита от несанкционированной модификации используемых программных средств, а также защита систем от внедрения вредоносных программ, включая компьютерные вирусы;

защита информации от утечки по техническим каналам связи при ее обработке, хранении и передаче;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, а также создание механизма оперативного реагирования на угрозы информационной безопасности;

реализация программ по осведомленности и обучению работников и обучающихся Университета о возможных рисках информационной безопасности и мерах противодействия.

ГЛАВА 3
ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

10. Система защиты информации Университета основывается на следующих принципах:

10.1. Законность – разработка, внедрение и функционирование системы защиты информации осуществляются в строгом соответствии с требованиями законодательства Республики Беларусь, а также иными нормативными правовыми актами в области защиты информации.

10.2. Системность – подход к обеспечению информационной безопасности является комплексным и охватывает все взаимосвязанные элементы информационных систем, включая персонал, программное обеспечение, технические средства и данные, а также учитывает все возможные факторы, способные оказать влияние на безопасность.

10.3. Комплексность – для противодействия угрозам информационной безопасности применяется совокупность согласованных правовых, организационных и технических мер, обеспечивающих многоуровневую защиту информационных активов на всех этапах их жизненного цикла.

10.4. Непрерывность – защита информации является непрерывным процессом, включающим постоянный мониторинг состояния защищенности, анализ актуальных угроз и уязвимостей, а также своевременную адаптацию и совершенствование мер защиты.

10.5. Своевременность – меры по обеспечению информационной безопасности носят упреждающий характер и направлены на предотвращение возможных инцидентов, а не только на реагирование на уже свершившиеся факты.

10.6. Экономическая целесообразность – затраты на создание и эксплуатацию системы защиты информации должны быть соразмерны ценности защищаемых информационных активов и величине возможного ущерба от реализации угроз информационной безопасности.

10.7. Обоснованность – используемые средства и методы защиты информации должны быть обоснованы с точки зрения установленного уровня безопасности и реализованы на базе современных достижений науки и техники.

10.8. Специализация и профессионализм – эксплуатация технических средств и реализация мер по защите информации должны осуществляться профессионально подготовленными работниками, обладающими необходимыми знаниями и квалификацией.

10.9. Взаимодействие и координация – обеспечение информационной безопасности достигается за счет четкого взаимодействия между структурными подразделениями Университета, координации их усилий и, при необходимости, сотрудничества с внешними организациями и государственными органами.

10.10. Личная ответственность – каждый работник, обучающийся и иной пользователь информационных систем Университета несет персональную ответственность за соблюдение установленных правил и требований информационной безопасности в пределах своей компетенции и полномочий.

РАЗРАБОТАЛИ

Специалисты по защите информации С.В.Курашов

А.В.Прохоренко

Декан факультета управления
и инноваций И.И.Маковецкий

СОГЛАСОВАНО

Первый проректор Ю.В.Машин

Проректор С.Л.Шабунин

Ведущий юрисконсульт Э.Ю.Карелин