Приложение 1

Учреждение образования
«Гомельский государственный
медицинский университет»

УТВЕРЖДЕНО
Приказ ректора университета
09.06.2025 № 284

ПОЛИТИКА
информационной безопасности

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика информационной безопасности (далее – Политика) учреждения образования «Гомельский государственный медицинский университет» (далее – Университет) разработана на основании Закона Республики Беларусь «Об информации, информатизации и защите информации», Закона Республики Беларусь «О защите персональных данных» и иных нормативных правовых актов Республики Беларусь в области информационной безопасности.

2. Политика распространяется на все структурные подразделения, работников и обучающихся Университета, а также лиц, участвующих в эксплуатации, обслуживании, поддержке объектов информационной системы (далее – ОИС), прикладного и системного программного обеспечения (далее – ПО), информационных ресурсов (далее – ИР), информационных систем Университета (далее – ИСУ).

3. Настоящая Политика является основным локальным правовым актом (далее – ЛПА) Университета, регулирующим вопросы информационной безопасности (далее – ИБ) в ИСУ. Иные ЛПА Университета в области ИБ уточняют и дополняют положения Политики ИБ с учетом детализации конкретных аспектов обеспечения ИБ Университета.

4. Общее руководство системой ИБ, принятие всех решений по вопросам ее функционирования, а также контроль за организацией работы по обеспечению ИБ возлагается на ректора. На проректоров возлагается ответственность за обеспечение ИБ по направлениям их деятельности в соответствии с распределением обязанностей.

5. Организационные и технические работы по обеспечению ИБ компьютерной сети Университета выполняет центр инновационных технологий (далее – ЦИТ) в соответствии с ЛПА, устанавливающими порядок осуществления деятельности по ИБ в Университете. В Университете обеспечивается наличие лиц, обладающих необходимой квалификацией и прошедших соответствующее обучение, а также повышение квалификации в установленном порядке.

ПРИНЦИПЫ И ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

6. Политика Университета по обеспечению ИБ направлена на защиту ИСУ от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИСУ, а также минимизация рисков ИБ.

7. Основными целями Политики ИБ являются:

снижение уровня рисков, связанных с ИБ;

снижение числа инцидентов, связанных с ИБ;

повышение компетентности работников в области ИБ;

улучшение имиджа Университета и минимизация ущерба вследствие возможного возникновения инцидентов ИБ и кибербезопасности;

обеспечение непрерывности бизнес-процессов;

обеспечение соответствия требованиям законодательства, стандартам и договорным обязательствам в части ИБ и защиты персональных данных.

8. Достижение указанных целей осуществляется посредством выполнения следующих мероприятий:

реализация требований законодательства Республики Беларусь в области ИБ;

своевременное выявление и оценка угроз ИБ, причин и условий, способствующих нанесению ущерба ИСУ и, как следствие, нарушению нормального функционирования Университета;

минимизация ущерба, который может быть нанесен Университету из-за нарушений ИБ ИСУ;

организация разграничения доступа пользователей к ИСУ (доступ пользователей только к тем информационным ресурсам и выполнению только тех операций в ИСУ, которые необходимы пользователям для выполнения служебных обязанностей);

обеспечение аутентификации пользователей ИСУ;

обеспечение регистрации действий пользователей ИСУ в системных журналах и организация контроля этих действий путем анализа содержимого журналов;

обеспечение защиты от несанкционированной модификации используемого в ИСУ ПО, а также защиты ИСУ от внедрения несанкционированных программ, включая вредоносное ПО;

обеспечение резервирования и архивирования информационных ресурсов;

обеспечение криптографической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче посредством сетей электросвязи общего пользования.

9. Построение системы защиты информации и ее функционирование должно осуществляться в соответствии со следующими принципами:

законность: предполагает осуществление мероприятий и разработку системы ИБ в соответствии с действующим законодательством Республики Беларусь;

системность: подход к построению системы ИБ, предполагающий учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ;

комплексность: комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты;

непрерывность: подход к построению системы ИБ, предполагающий принятие мер ИБ на всех этапах жизненного цикла ИСУ;

своевременность: подход к построению системы ИБ, предполагающий упреждающий характер мер ИБ для обеспечения безопасности информации;

преемственность и совершенствование: предполагают постоянное совершенствование мер ИБ и средств защиты информации (далее – СрЗИ);

экономическая целесообразность: предполагает соответствие уровня затрат на обеспечение ИБ ценности информационных ресурсов по отношению к величине возможного ущерба при нарушениях функционирования ИСУ;

персональная ответственность: предполагает возложение ответственности за обеспечение ИБ на каждого работника в пределах его полномочий;

принцип минимизации полномочий: означает предоставление пользователям ИСУ минимальных прав доступа в соответствии с производственной необходимостью;

техническая реализуемость: средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

СУБЪЕКТЫ, ОБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ И ПОРЯДОК ИХ ВЗАИМОДЕЙТСВИЯ

10. Субъектами информационных отношений являются:

лица, осуществляющие обеспечение безопасного использования ИР, ИС и ОИС;

иные работники и профессорско-преподавательский состав Университета, получивший доступ к ИР, ИС и ОИС Университета и

использующий их в рамках выполнения своих должностных обязанностей;

посетители Университета;

должностные лица организаций, поставляющие ИР, ИС и ОИС для Университета и осуществляющие их гарантийное и сервисное обслуживание.

11. Ответственность Субъектов за обеспечение защиты информации в Университете установлена в следующих документах:

организационно-распорядительных документах;

должностных инструкциях работников Университета в обязанности которых входит обеспечение защиты ИС.

иных документах, в том числе в иных локальных правовых актах, а также в соглашениях и договорах.

12. Объектами информационных отношений являются:

информация, хранящаяся и обрабатываемая в ИСУ;

процессы обработки информации, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

средства вычислительной техники и другая ИТ-инфраструктура ИСУ, включающая технические и программные средства обработки, передачи и отображения информации, каналы информационного обмена;

помещения и другая инфраструктура (системы электропитания, кондиционирования, пожаротушения, система контроля управления доступом и т.д.) Университета, необходимые для безопасного и бесперебойного функционирования ИСУ.

13. Порядок информационного взаимодействия Объектов между собой определяется соответствующей эксплуатационной документацией.

14. Основными составляющими Объектами являются компоненты, входящие в состав информационной инфраструктуры Университета:

локальная вычислительная сеть;

информационные системы;

отдельные рабочие места, предназначенные для доступа, хранения и обработки информации, не отнесенной к государственным секретам, распространение и (или) предоставление которой ограничено.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

15. Система управления ИБ (далее – СУИБ) Университета функционирует на основе процессной модели, предусматривающей непрерывный цикл мероприятий (планирование, реализация, проверка, действие), направленных на постоянное совершенствование деятельности по обеспечению ИБ.

16. При планировании и реализации мероприятий по обеспечению ИБ осуществляются:

инвентаризация объектов и информационных ресурсов ИСУ и уточнение состава ИСУ;

оценка важности (категорирование) объектов и информационных ресурсов ИСУ;

оценка рисков для ИСУ (при необходимости) согласно СТБ 34.101.70-2016 «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах», либо по методике, разрабатываемой Университетом;

проектирование, внедрение и поддержание в актуальном состоянии СЗИ ИСУ;

разработка и поддержание в актуальном состоянии ЛПА СЗИ ИСУ по вопросам ИБ;

обучение работников Университета вопросам ИБ.

17. Для проверки соответствия СУИБ требованиям законодательства о защите информации, оценки степени (качества) защиты Университета от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на ИСУ, проводятся периодические аудиты ИБ.

18. В процессе эксплуатации ИСУ осуществляются:

контроль за соблюдением требований, установленных в ЛПА СЗИ ИСУ в области ИБ;

контроль за порядком использования ИСУ;

мониторинг функционирования ИСУ и используемых СрЗИ;

выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования ИСУ;

резервное копирование информации, содержащейся в ИСУ;

выявление и фиксация инцидентов ИБ, принятие мер по своевременному реагированию на инциденты ИБ, выполнению мероприятий по недопущению инцидентов ИБ.

19. На основе анализа функционирования СУИБ осуществляется выявление и фиксация нарушений требований по защите информации, принимаются меры по своевременному устранению таких нарушений.

В случае несоответствия уровня защищенности ИСУ требованиям законодательства в сфере ИБ, изменения требований законодательства, производится корректировка СЗИ ИСУ.

20. Организационная схема СУИБ приведена в Приложении 1 к Политике ИБ.

В случае несоответствия уровня защищенности ИСУ требованиям законодательства в сфере ИБ, изменения требований законодательства, производится корректировка СЗИ ИСУ.

21. Ректор Университета своим приказом назначает проректора по

безопасности, режиму и кадрам ответственным за организацию работы по обеспечению информационной безопасности Университета.

22. В подчинении проректора по безопасности, режиму и кадрам находится инженер по защите информации. Он возглавляет функциональное руководство ИБ Университета, в состав которого входят руководители всех структурных подразделений Университета, входящих в границы ИСУ.

РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

23. Субъекты имеют необходимый уровень доступа к Объектам Университета, назначенный в соответствии с принципом минимизации прав, назначаемых пользователям. Доступ к ИСУ предоставляется пользователям только в объеме, необходимом для выполнения должностных обязанностей.

24. Порядок и правила предоставления доступа к Объектам Университета определяются следующими документами:

настоящей Политикой;

договорами при оказании Университету услуг, в том числе технической поддержки;

должностными и рабочими инструкциями работников;

иными локальными правовыми актами Университета.

ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ (ПОЛЬЗОВАТЕЛЕЙ) ИНФОРМАЦИОННЫХ СИСТЕМ

25. Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений имеют право:

использовать ОИС для доступа к ИС и ИР, другим ОИС с целями поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления и пользования информацией;

осуществлять иные действия в соответствии с должностными инструкциями и ЛПА Университета.

26. Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений обязаны:

соблюдать права других лиц при использовании Объектов Университета;

соблюдать надежность пароля (базовые требования: длина пароля - не менее восьми символов; алфавит - кириллица, латиница, цифры, специальные символы; плановая смена пароля - не реже одного раза в квартал) для предотвращения взлома;

хранить пароль в месте, исключающем его компрометацию другими пользователями и иными лицами;

запрещено предоставлять иным лицам пароль от личной учётной записи. Обладателем пароля к личной учётной записи является только его пользователь;

запрещается переходить по активным ссылкам в письмах, полученных из неизвестных (ненадёжных) источников;

исполнять обязанности в соответствии с должностными инструкциями и ЛПА Университета;

не допускать открытия гиперссылок из ненадёжных источников («зловредных ссылок») при использовании корпоративных и личных почтовых ящиков на рабочих местах;

27. Ректор Университета для обеспечения защиты информации в ИСУ:

определяет цели, внутренние и внешние границы обеспечения ИБ ИСУ с учетом стратегических целей Университета;

распределяет среди работников Университета функции по обеспечению ИБ ИСУ;

определяет ответственность работников Университета за конкретные аспекты обеспечения ИБ ИСУ;

определяет временные рамки и последовательность реализации мероприятий по обеспечению ИБ ИСУ;

определяет перечень и объем ресурсов, которые могут быть задействованы для обеспечения ИБ ИСУ;

утверждает и вводит в действие (приказом) ЛПА Университета в области ИБ;

дает оценку эффективности ИБ, реализованных в ИСУ.

28. Проректор по безопасности, режиму и кадрам в рамках реализации требований Политики ИБ:

обеспечивает координацию действий всех структурных подразделений и работников Университета, входящих в границы ИСУ, при реализации требований Политики ИБ;

организовывает разработку и согласовывает ЛПА СЗИ ИСУ в области ИБ;

организовывает и внедряет процессы ИБ в Университете;

организовывает внедрение и эксплуатацию СрЗИ в ИСУ;

организовывает мониторинг ИБ Университета;

формирует группу реагирования на инциденты ИБ ИСУ и контролирует ее работу;

утверждает отчетные документы по результатам мониторинга, аудита ИБ и реагирования на инциденты ИБ в ИСУ;

информирует ректора о состоянии ИБ в Университете.

29. Инженер по защите информации в рамках реализации требований Политики ИБ:

осуществляет контроль за соблюдением правил разграничения доступа пользователей к ИСУ, за соблюдением правил генерации и смены паролей доступа пользователей, определяет конфигурацию СрЗИ и средств криптографической защиты информации (далее – СКЗИ) и в рамках реализации требований Политики ИБ:

осуществляет настройку и эксплуатацию СрЗИ и СКЗИ в ИСУ;

совместно с администратором сетей проводит мероприятия, позволяющие выявлять вредоносное ПО в ИСУ, обновление и настройку имеющегося ПО;

совместно с администратором сетей принимает меры по восстановлению работоспособности ИСУ при любых инцидентах, связанных с нарушением ИБ ИСУ;

выполняет работы по анализу инцидентов ИБ ИСУ, реагированию на них, планирует и обеспечивает контроль за исполнением мероприятий по недопущению аналогичных инцидентов в будущем;

разрабатывает предложения по актуализации ЛПА СЗИ ИСУ, регламентирующих ИБ;

осуществляет мониторинг ИБ ИСУ, включая соблюдение требований ИБ при настройке программных и программно-аппаратных средств.

30. Администратор сетей в рамках реализации требований Политики ИБ:

создает учетные записи пользователей в ИСУ, производит изменения учетных записей при переходе работников Университета из одного подразделения в другое или при окончании работы в нем;

осуществляют поддержание работоспособности ИСУ с учетом требований Политики и иных ЛПА СЗИ ИСУ в области ИБ;

осуществляет корректное применение доступных механизмов защиты информации в ИСУ в соответствии с настоящей Политикой ИБ;

уведомляет инженера по защите информации об эффективности применяемых в ИСУ методов обеспечения ИБ и любых технических соображениях, которые могли бы улучшить эффективность ИБ в ИСУ;

информирует пользователей о запланированном прекращении работы ИСУ, а также о предполагаемых сроках восстановления ее работоспособности;

осуществляют своевременную проверку системных журналов серверов ИСУ с целью выявления нарушений ИБ (предпосылок к таким нарушениям);

осуществляет мониторинг функционирования ИСУ;

принимает меры по восстановлению работоспособности ИСУ при любых инцидентах ИБ;

своевременно информирует инженера по защите информации о каждом инциденте ИБ ИСУ.

31. Начальники структурных подразделений Университета в рамках реализации требований Политики ИБ:

осуществляют мониторинг состояния ИБ в подчинённых им подразделениях Университета, входящих в границы ИСУ, и своевременно информируют инженера по защите информации и (или) администратора сетей об инцидентах ИБ ИСУ;

организовывают обучение по вопросам ИБ ИСУ и контроля навыков работников в области ИБ в подчинённых им подразделениях;

принимают участие в работе группы реагирования на инциденты ИБ ИСУ;

разрабатывают необходимые отчетные документы при проведении аудитов ИБ.

Начальники структурных подразделений Университета несут персональную ответственность за состояние ИБ ИСУ в подчинённых им подразделениях.

32. Пользователь АРМ в рамках реализации требований Политики ИБ:

использует ИСУ исключительно в служебных целях;

знает и выполняет правила использования ИСУ, определенные настоящей Политикой ИБ и иными ЛПА СЗИ ИСУ в области ИБ;

использует доступные механизмы ИБ для защиты конфиденциальности и целостности собственной информации, когда это требуется;

выбирает и использует пароли в соответствии с требованиями ЛПА СЗИ ИСУ по вопросам ИБ;

немедленно уведомляет инженера по защите информации и (или) администратора сетей о возможной компрометации паролей авторизованного доступа к ИСУ;

своевременно уведомляет инженера по защите информации и (или) администратора сетей о нарушении ИБ или обнаруженном отказе ИСУ;

использует ПО и программно-аппаратные средства защиты, которые доступны в ИСУ, для защиты от вредоносного ПО;

блокирует доступ к ИСУ при уходе с рабочего места (в том числе в течение рабочего дня) для предотвращения использования ИСУ неавторизованными пользователями.

Пользователю АРМ запрещается осуществлять любые попытки неавторизованного доступа к ресурсам ИСУ, в том числе и от имени других авторизованных пользователей.

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ УНИВЕРСИТЕТА С ИНЫМИ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И СИСТЕМАМИ

33. Порядок взаимодействия Объектов Университета с иными ИС определяется действующим законодательством и соответствующими документами по каждому взаимодействию.

34. Функционирование Объектов Университета осуществляется с обновлением системного, прикладного ПО и антивирусных баз из доверенных источников.

35. Обновление баз средств защиты информации от действий вредоносного ПО и файлов осуществляется с периодичностью, установленной производителем антивирусного ПО.

36. Доступ к сети Интернет предоставляется только авторизованным сервисам и пользователям.

37. К авторизованным сервисам Университета относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление баз СрЗИ от действий вредоносного ПО и файлов.

38. При необходимости организации дистанционной работы в ИСУ разрабатывается перечень информационных ресурсов (сервисов) ИСУ, доступ к которым необходим для исполнения должностных обязанностей работниками, осуществляющими дистанционную работу.

На основании Перечня ресурсов (сервисов) ИСУ, доступ к которым необходим для исполнения должностных обязанностей работниками, осуществляющими дистанционную работу, осуществляется проектирование и создание системы удаленного доступа к ИСУ.

Для обеспечения удаленного доступа к ИСУ могут применяться дополнительные средства (методы) аутентификации пользователей ИСУ.

ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

39. Работники и обучающиеся Университета, а также привлекаемые лица, участвующие в эксплуатации, обслуживании, поддержке объектов ОИС, ПО, ИР, ИС Университета несут персональную ответственность за соблюдение требований настоящей Политики.

40. Неисполнение или некачественное исполнение работниками Университета, обучающимися, пользователями ИСУ обязанностей по обеспечению ИБ может повлечь лишение доступа к информационным ресурсам, а также применение к виновным мер воздействия, вид и степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

41. В развитие настоящей Политики могут приниматься локальные правовые акты Университета.

42. В случае изменения действующего законодательства, а также Устава Университета, настоящая Политика применяется в части, не противоречащей вновь принятым нормативным правовым актам, а также Уставу Университета.

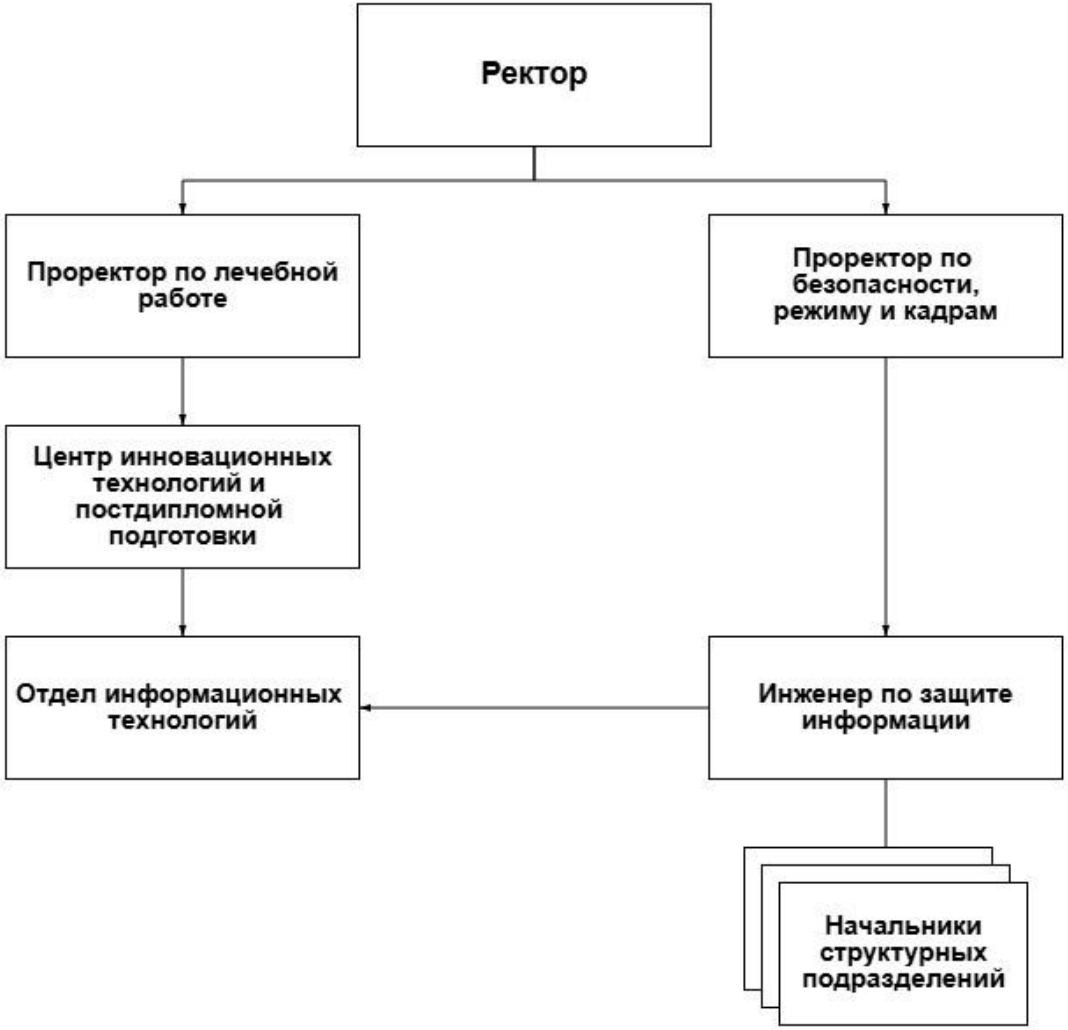
43. При необходимости внесении изменений в настоящую Политику, изменения в существующий документ не вносятся, она переиздается и утверждается заново.

44. Плановое изменение настоящей Политики должно осуществляться не реже одного раза в год.

45. Внеплановое изменение настоящей Политики может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.

46. Пересмотр настоящей Политики инициируется проректором по безопасности, режиму и кадрам (в случае планового изменения) или инженером по защите информации (в случае внепланового изменения).

47. Пересмотр настоящей Политики согласовывается с проректором по безопасности, режиму и кадрам, после чего утверждаются ректором.

Приложение 1

Организационная схема СУИБ Университета