

УТВЕРЖДЕНО

Приказ ректора академии

11.12.2023 № 79

## ПОЛИТИКА

информационной безопасности  
учреждения образования  
«Белорусская государственная  
академия музыки»

ГЛАВА 1  
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности (далее – Политика) учреждения образования «Белорусская государственная академия музыки» (далее – академия) разработана в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (далее – Положении о технической и криптографической защите информации).

Нормативной правовой основой Политики служат:

Гражданский кодекс Республики Беларусь;

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»;

постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь»;

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 реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

иные нормативные правовые акты Республики Беларусь в области информатизации, безопасности и защиты информации, международные стандарты в области информационной безопасности продуктов и систем информационных технологий.

2. Политика определяет общие цели и принципы деятельности по защите академии от возможного нанесения материального, физического

или иного ущерба посредством случайного или преднамеренного воздействия на информационные системы (далее – ИС), а также минимизации рисков информационной безопасности (далее – ИБ).

3. Настоящая Политика не охватывает вопросы защиты информации, отнесенной к государственным секретам. Защита данного вида информации регламентируется соответствующими нормативными правовыми актами.

4. Положения Политики доводятся до ознакомления и являются обязательными для работников структурных подразделений академии, организующих и обеспечивающих эксплуатацию ИС при выполнении своих трудовых обязанностей, абитуриентов и обучающихся академии, взаимодействующих с ИС в процессе поступления и обучения в академии, иных пользователей ИС, физических или юридических лиц, выступающих в качестве информационных посредников, операторов информационных систем и связи.

5. Политика должна актуализироваться в связи с изменением в законодательстве Республики Беларусь в области защиты информации, изменениями в организационной структуре или в информационной инфраструктуре академии, но не реже одного раза в год. Поддержание положений Политики в актуальном состоянии осуществляет отдел информационных технологий (далее – ОИТ).

## ГЛАВА 2 ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

6. Для целей Политики применяются термины в значениях, определенных Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, Законе Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7 мая 2021 г. № 99-3 «О защите персональных данных», а также следующие термины и их определения:

администрирование ИС - это предоставление пользователям соответствующих прав использования возможностей работы с ИС и обеспечение целостности данных;

активы – информация или ресурсы, которые должны быть защищены средствами системы защиты информации, используемыми в ИС;

анализ риска – систематическое использование информации для выявления источников и оценки степени риска;

атака – попытка нарушения ИБ или попытка обхода средств управления безопасностью ИС;

аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;

доступность – свойство активов ИС, заключающееся в возможности их использования по требованию субъекта, имеющего соответствующие полномочия, за приемлемое время;

информационная безопасность – состояние защищенности информации и бизнес-процессов академии, объединяющих в своем составе работников и обучающихся академии, от внешних и внутренних угроз в информационной сфере;

информационная система – совокупность банков данных, информационных технологий и комплекса программно-технических средств (далее – КПТС), применяемых для обеспечения бизнес-процессов академии;

инцидент информационной безопасности – одно или ряд нежелательных, или непредвиденных событий в области ИБ, при которых имеется значительная вероятность компрометации функционирования деловых процессов или реализации угрозы ИБ;

комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

контролируемая зона – территория вокруг объекта информатизации, здание, часть здания, в пределах которого исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих разрешения на постоянный или разовый доступ на объект;

конфиденциальность – свойство информации, обрабатываемой ИС, быть недоступной и закрытой от раскрытия и использования пользователями, лицами, логическими объектами или процессами ИС, которые не имеют соответствующих полномочий;

критический ресурс – объекты информационной сети, несанкционированный доступ к которым может повлечь за собой доступность информационных систем;

пользователь ИС – физическое лицо, обладающее правом доступа к ИС;

риск ИБ – потенциальная возможность реализации угроз ИБ, которая может повлечь нарушение или прекращение функционирования ИС;

система защиты информации (далее – СЗИ) – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС академии;

событие ИБ – идентифицированное возникновение состояния ИС, услуги или сети, указывающее на возможное нарушение ИБ или отказ средств защиты, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

целостность – свойство сохранения полноты состава и неизменности активов ИС;

угроза – описание возможности воздействия на ИС в понятиях источник угроз (нарушитель), атака и актив, который подвергается атаке.

### ГЛАВА 3 ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

7. Целями защиты информации является защита академии от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

8. Основными задачами академии в части обеспечения безопасности информации в ИС являются:

реализация требований законодательства Республики Беларусь в части информационной безопасности ИС и мер контроля их защищенности; определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности академии;

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

разграничение доступа пользователей к ИС (предоставление доступа пользователям только к тем информационным ресурсам и выполнению только тех операций в ИС, которые необходимы пользователям для выполнения своих служебных обязанностей);

обеспечение аутентификации пользователей;

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

обеспечение защиты от несанкционированной модификации используемого в ИС программного обеспечения (далее – ПО), а также защиты ИС 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;

своевременное выявление и оценка причин, условий и характера угроз ИБ, дальнейшее прогнозирование и профилактика развития событий ИБ на основе мониторинга инцидентов ИБ;

выявление, предупреждение и пресечение возможности противоправной и иной деятельности работников и обучающихся академии;

планирование, реализация и контроль эффективности использования защитных мер и СЗИ, создание механизма оперативного реагирования на угрозы ИБ; реализация программ по осведомленности работников академии о возможных факторах рисков ИБ и мерах противодействия.

#### ГЛАВА 4 СУБЪЕКТЫ И ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

9. Субъектами информационной безопасности являются:

ответственные за ИБ в ИС – должностные лица академии или структурные подразделения, обеспечивающие ИБ в той или иной ИС, определенные в пунктах 34 – 44 настоящей Политики;

ответственное подразделение по защите сетевой инфраструктуры академии – структурное подразделение, организующее внедрение и функционирование технической системы ИБ, имеющее в составе специалистов, выполняющих функции администратора ИБ ИС. Ответственным подразделением по информационной безопасности академии является отдел информационных технологий;

ответственное лицо по структурным подразделениям академии – работники отдела информационных технологий, обеспечивающие корректное и безопасное функционирование ИС, компьютеров и сети структурных подразделений академии, и выполняющие функции системного администратора.

пользователи ИС – работники, обучающиеся, абитуриенты академии, использующие ИС для решения задач, возникающих в процессе выполнения должностных обязанностей, обучения или поступления в академию.

10. При планировании и реализации мероприятий по обеспечению ИБ в академии осуществляются:

инвентаризация информационных ресурсов академии и уточнение состава ИС;

оценка важности (категорирование) информационных ресурсов и элементов ИС;

формирование методики оценки рисков (установление критериев рисков для ИС и информационных ресурсов академии и формирование методики обработки рисков);

внедрение и поддержание в актуальном состоянии СЗИ;

разработка и поддержание в актуальном состоянии локальных правовых актов академии по вопросам ИБ;

консультирование пользователей ИС по вопросам ИБ.

11. Для проверки соответствия системы управления ИБ требованиям законодательства о защите информации, оценки степени (качества) защиты академии от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС проводятся периодические аудиты ИБ согласно документации системы защиты информации.

12. В процессе эксплуатации ИС осуществляются:

контроль за соблюдением требований, установленных локальными правовыми актами академии в области ИБ;

контроль за порядком использования ИС;

мониторинг функционирования ИС и СЗИ;

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

резервное копирование информации, содержащейся в ИС;

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

13. На основе анализа функционирования системы управления ИБ в ходе эксплуатации ИС осуществляется постоянная оценка соответствия уровня защищенности ИС установленным критериям риска.

В случае несоответствия заданным критериям или их изменения производится корректировка СЗИ ИС.

14. Объектами ИБ являются:

информация, хранящаяся и обрабатываемая в ИС академии, а также передаваемая в академию при оказании услуг (классификация информации, хранящейся и обрабатываемой в ИС академии, представлена в разделе Перечень информационных систем);

КПТС, включающий технические, программные и программноаппаратные средства обработки, передачи и отображения информации, в том числе каналы передачи данных и информационного обмена, средства технической и криптографической защиты информации.

15. Основными составляющими КПТС академии являются компоненты, входящие в состав корпоративной информационной сети академии:

- центр обработки данных (далее – ЦОД);
- коммуникационная инфраструктура;
- информационные системы;
- программное обеспечение, в том числе обеспечивающее функционирование ЦОД и коммуникационной инфраструктуры;
- автоматизированные рабочие места работников и студентов.

16. КПТС должен располагаться в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

17. Порядок информационного взаимодействия субъектов с объектами информационной безопасности академии определяется локальными правовыми актами.

18. Порядок информационного взаимодействия объектов между собой определяется эксплуатационной (технической) документацией на ИС академии.

## ГЛАВА 5 ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

19. ИБ академии базируется на принципах конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС академии.

20. Необходимый уровень безопасности достигается путем реализации мер, направленных на минимизацию возможного ущерба за счет:

- профилактики нарушения ИБ;
- своевременного обнаружения нарушений ИБ;
- эффективного восстановления нормального состояния ресурсов и функционирования ИС.

21. Обеспечение целостности и конфиденциальности информации и информационных ресурсов ИС достигается:

- управлением доступом пользователей к информации;
- резервным копированием информации и резервированием инфраструктуры;

контролем действий пользователей, в частности действий, производимых с критическими ресурсами, влияющими на работоспособность ИС;

наличием антивирусной защиты в составе СЗИ;

средствами криптографической защиты информации (при необходимости).

22. Доступность информационных ресурсов и услуг ИС пользователям обеспечивается:

резервированием аппаратных и программных средств ИС;

наличием регулярно актуализируемых и проверенных на практике планов обеспечения непрерывной работы и восстановления ИС;

наличием соглашения с оператором сети Интернет об уровне предоставления сервиса, содержащим описание услуги, права и обязанности сторон, согласованный уровень качества предоставления услуги (доступность, надежность, безопасность и управляемость); наличием документированных процедур, регламентирующих процессы жизненного цикла программно-технических средств, направленных на обеспечение непрерывности функционирования ИС.

23. Подлинность пользователя ИС достигается за счет средств аутентификации ИС.

24. Сохранность информационных ресурсов и услуг ИС достигается за счет системы хранения данных и реализации резервного копирования.

25. Управление инцидентами ИБ осуществляется в соответствии с установленными правилами управления инцидентами ИБ в ИС.

26. Для всех критических ресурсов определяются правила, установленные Положением о копировании, резервировании и восстановлении информации.

27. Порядок и правила предоставления доступа к объектам информационной безопасности академии определяется локальными правовыми актами.

28. Работникам академии предоставляется уровень доступа к объектам ИБ академии в объеме, необходимом для выполнения своих должностных обязанностей.

29. Физический доступ к КППТС (охраняемые зоны, периметры безопасности и, т.п.) обеспечивается в соответствии с Инструкцией о порядке организации доступа в серверные помещения академии.

Технические средства защиты оборудования должны включать в себя источники бесперебойного питания и кондиционеры.

30. Работы в серверных помещениях должны производиться по согласованию с ответственным подразделением по ИБ и под контролем

должностных лиц, выполняющих функции ответственного лица по структурным подразделениям академии.

31. Размещение ИС, обрабатывающих информацию ограниченного распространения, в виртуальной инфраструктуре центров обработки данных сторонних организаций, предоставляющих соответствующие услуги, должно производиться исключительно при условии выполнения данными организациями требований законодательства Республики Беларусь в сфере защиты информации и по согласованию с ОИТ.

## ГЛАВА 6 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

32. Пользователи ИС должны:

осуществлять любые действия в ИС, к которым предоставлен доступ, после авторизации с использованием персональной учетной записи, зарегистрированной в ИС академии;

использовать персональные компьютеры исключительно для тех целей, для которых они были предоставлены;

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

устанавливать и использовать пароли в соответствии с требованиями локальных правовых актов по вопросам ИБ;

немедленно уведомлять ответственное лицо по структурному подразделению или ответственное подразделение за ИБ о возможной компрометации паролей авторизованного доступа к ИС;

блокировать доступ к ИС при уходе с рабочего места для предотвращения использования ИС неавторизованными пользователями.

33. Любое использование оборудования для целей, не связанных со служебной деятельностью либо целями обучения, расценивается как несанкционированное использование оборудования.

Несанкционированная деятельность субъектов ИБ может обнаруживаться любыми незапрещенными законодательством способами и должна незамедлительно пресекаться.

## ГЛАВА 7 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

34. В академии функционируют следующие ИС:

электронный почтовый сервис;

официальный сайт академии;

репозиторий;

«Система документооборота»;

«Система межведомственного документооборота»;  
«Электронная библиотека»;  
«База-сироты»;  
«Студент»;  
«1С: Кадры»;  
«1С: Бухгалтерия».

35. Для обеспечения работоспособности ИС используются структурированная кабельная система, сервера и соответствующее программное обеспечение. Для доступа к информационным системам используются персональные компьютеры, находящиеся во внутренней сети академии.

36. Для получения доступа к ИС и информационной сети академии сотрудник заполняет заявление установленного образца, визирует заявление проректор по безопасности, режиму и кадрам.

37. Электронный почтовый сервис, относится к классу 3-юл. Администрирование обеспечивает отдел информационных технологий. Доступ имеют все пользователи информационной сети академии. Информационную безопасность данной ИС осуществляют отдел информационных технологий и обслуживающая организация, и/или разработчики, и/или обслуживающая организация при технической поддержке отдела информационных технологий.

38. ИС «Система документооборота» относится к классу 3-юл. Администрирование ИС осуществляет отдел информационных технологий. Доступ к ИС «Система документооборота» работники академии получают по докладной записке на имя проректора по безопасности, режиму и кадрам. Информационную безопасность данной ИС осуществляют отдел информационных технологий и обслуживающая организация, и/или разработчики, и/или обслуживающая организация при технической поддержке отдела информационных технологий.

39. ИС «Электронная библиотека» относится к классу 3-ин. Администрирование ИС обеспечивает отдел информационных технологий. Доступ к ИС «Электронная библиотека» предоставляется всем пользователям информационной сети академии. Информационную безопасность данной ИС осуществляет отдел информационных технологий, и/или разработчики, и/или обслуживающая организация при технической поддержке отдела информационных технологий.

40. Главный сайт академии, доступный по адресу [bgam.by](http://bgam.by), относится к классу 5-гос. Администрирование обеспечивает отдел информационных технологий. Право на редактирование сайта академии предоставляется работнику, назначенному в установленном порядке

приказом ректора академии, путем направления информации через электронный почтовый сервис, в установленном порядке назначенными, пользователями академии, ответственными за соответствующий раздел сайта академии. Информационную безопасность данной ИС осуществляет отдел информационных технологий, и/или разработчики, и/или обслуживающая организация при технической поддержке отдела информационных технологий академии.

41. При разработке информационной системы, которая будет размещена в ЦОД академии (центральном сервере академии) либо в инфраструктуре академии, разработчики либо заинтересованное структурное подразделение обязаны разработать СЗИ в соответствии с действующим законодательством и согласовать с проректором по безопасности, режиму и кадрам.

42. Структурные подразделения, которые являются владельцами разработанных информационных систем, которые размещены в ЦОД академии (центральном сервере академии) либо в инфраструктуре академии, обязаны разработать СЗИ в соответствии с действующим законодательством по согласованию с проректором по безопасности, режиму и кадрам.

43. Технические аспекты защиты корпоративной сетевой инфраструктуры ЦОД академии (центрального сервера академии) возлагаются на проректора по безопасности, режиму и кадрам, отдел информационных технологий.

44. При увольнении работника все предоставленные пользователю права доступа к ресурсам ИС удаляются. При изменении трудовых отношений руководитель структурного подразделения уведомляет ОИТ с помощью докладной записки о лишении прав доступа работника академии к ИС, указанным в пунктах 37-39.

## ГЛАВА 8 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

45. Порядок взаимодействия объектов ИБ академии с ИС академии определяется локальными документами по каждому взаимодействию.

46. Обновление баз средств антивирусной защиты информации должно осуществляться с периодичностью, рекомендованной производителем антивирусного программного обеспечения.

47. Правила доступа к корпоративной информационно-коммуникационной сети регулируются приказом ректора.

48. Синхронизация времени программных средств коммутационного оборудования, компьютеров, серверов, центра

обработки данных (далее – объекты академии) осуществляется ежедневно в автоматическом режиме.

49. Функционирование объектов академии должно осуществляться с синхронизацией времени с Интернет-ресурсом Белорусского государственного института метрологии belgim.by и обновлением системного, прикладного программного обеспечения и антивирусных баз с соответствующими ресурсами.

50. К авторизованным сервисам академии относятся:  
обновление системного и прикладного ПО;  
обновление встроенного ПО техническим средствам;  
обновление антивирусных средств защиты информации;  
синхронизация времени с источником надежного времени.

51. Взаимодействие объектов академии с иными ИС определяются соответствующими документами. Для взаимодействия объектов академии с иными ИС должны применяться СЗИ, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы при Оперативно-аналитическом центре при Президенте Республики Беларусь.

## ГЛАВА 9 ПОРЯДОК ОРГАНИЗАЦИИ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ В ХОДЕ ДИСТАНЦИОННОЙ РАБОТЫ

52. Профессорско-преподавательскому составу академии и работникам, принятым на дистанционную работу в академию, предоставляется автоматический доступ для дистанционной работы с распределенной автоматической ИС при помощи технологии VPN.

53. Для организации дистанционной работы при помощи технологии VPN руководители (начальники) структурных подразделений формируют списки работников, ИС и ресурсов (сервисов) академии с обоснованием необходимости дистанционной работы.

54. Организацию и согласование удаленного доступа при помощи технологии VPN к ИС академии осуществляет ОИТ исключительно при использовании оборудования принадлежащего академии. Если есть возможность рисков ИБ академии, то ОИТ вправе отказать в удаленном доступе к ИС академии.

55. Для обеспечения дистанционной работы при помощи технологии VPN с ИС академии и ресурсами (сервисами) академии,

ОИТ вправе создавать дополнительные средства (методы) аутентификации работников академии.