Приложение

УТВЕРЖДЕНА
приказом РАМ имени Гнесиных
«15» июля 2026 г. № 1220

ПОЛИТИКА

защиты информации и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия музыки имени Гнесиных»

1. Вводные положения

Настоящий документ определяет Политику информационной безопасности и защиты информации (далее – Политика) федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия музыки имени Гнесиных» (далее – РАМ имени Гнесиных, Академия).

Политика разработана во исполнение пункта 14 Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11.04.2025 № 117 (далее – Приказ № 117 и/или Требования), и определяет перечень защищаемых информационных систем, цели защиты информации, а также обязанности работников по обеспечению защиты информации.

Политика выражает позицию Академии в области защиты информации и информационной безопасности, систему взглядов, принципов и подходов в этой области для обеспечения защищенности образовательных, научных, исследовательских, финансово-хозяйственных и иных процессов Академии, направленных на достижение целей, предусмотренных Уставом РАМ имени Гнесиных, создания условий безопасного цифрового развития Академии и обеспечения соответствия требованиям законодательства Российской Федерации в данной области.

Политика Академии разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности и защиты информации, с учетом передового опыта и лучших практик.

На основании Политики Академии разрабатываются и утверждаются внутренние стандарты и регламенты по защите информации и информационной безопасности.

Область действия

Требования Политики Академии распространяются на:

– информационные системы Академии, включая программные и программно-аппаратные средства, информационные ресурсы и информацию, обрабатываемую в Академии, за исключением сведений, составляющих государственную тайну;

– информационно-технологическую инфраструктуру Академии, включая сервисы, телекоммуникационное оборудование и каналы связи, обеспечивающие передачу информации между информационными системами и информационное взаимодействие участников информационного обмена;

– системы и подсистемы защиты информации Академии, обеспечивающие реализацию и контроль мер информационной безопасности;

– работников Академии, участвующий в процессах сбора, накопления, систематизации, обработки, передачи, хранения и защиты информации.

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

Период действия и порядок внесения изменений

Политика Академии является локальным нормативным актом постоянного действия.

Политика Академии утверждается, изменяется и признается утратившей силу в Академии в соответствии с приказом ректора Академии.

2. Основные термины и сокращения

В настоящей Политике Академии применяются следующие основные термины и сокращения:

Контрагент	Текущие и потенциальные контрагенты Академии.
Информация	Сведения (сообщения, данные) независимо от формы их представления.

Информационный актив	Информационные системы и информационный ресурсы Академии, осуществляющие обработку информации автоматизированными и не автоматизированными средствами и имеющие ценность для Академии.
Информационно-технологическая инфраструктура	Комплексная структура, объединяющая все информационные системы, технологии и информационный ресурсы, используемые Академией. 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 Академии.
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 Академию. Статус абитуриента прекращается с момента зачисления в Академию.
Обучающийся	Физическое лицо, осваивающее образовательную программу в Академии.
Работник	Физическое лицо, вступившее в трудовые отношения с Академией.
Процессы Академии	Образовательные, научные, исследовательские, финансово-хозяйственные и иные процессы Академии, направленные на достижение целей, предусмотренных Уставом Академии.

Риск информационной безопасности (ИБ-риск)	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива.
Защита информации	Комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности 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.
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.

3. Заявление о Политике защиты информации и информационной безопасности

Принятием Политики Академия провозглашает и обязуется осуществлять все возможные меры для защиты работников, абитуриентов, обучающихся, контрагентов, а также имущества, информации, деловой репутации и Процессов Академии от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Академии 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 Академии. Соблюдение принципов информационной безопасности, защиты информации дополнительно позволит

упрочить конкурентные преимущества Академии, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить репутационные риски.

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

Руководство Академии придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является безусловным и необходимым элементом в работе Академии. 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 и научную деятельности, а также совместную работу с контрагентами Академии. Каждый работник Академии и его контрагенты несут ответственность за безопасную работу с вверенными им информационными активами, компьютерным оборудованием, виртуальной инфраструктурой, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Академии.

Работники ответственные за обеспечение защиты информации Академии должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищенности информации, информационных систем Академии, информационных активов, информационно-технологической инфраструктуры и Процессов Академии.

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

Контрагенты Академии должны быть проинформированы о Политике Академии, соблюдать ее положения, нести ответственность за их нарушение.

4. Цели и задачи Академии по защите информации и информационной безопасности

Управление и обеспечение информационной безопасности и защиты информации Академии ориентированы на достижение следующих целей в области информационной безопасности:

– предоставление безопасной информационной среды для функционирования и развития Процессов Академии;

– недопущение (исключение или снижение возможности до уровня, позволяющего осуществлять устойчивое цифровое развитие Академии) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

– недопущение (исключение или снижение возможности до уровня, позволяющего осуществлять устойчивое цифровое развитие Академии) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

Для достижения данных целей необходимо решение следующих задач:

– обеспечение защиты информации и информационной безопасности Процессов Академии включая обеспечение оперативного мониторинга и оценку состояния защищенности в Академии;

– обеспечение защиты информации от противоправных спланированных целенаправленных компьютерных атак и повышение эффективности защиты;

– повышение информационной безопасности технологических и образовательных систем;

– применение новых современных методов, обеспечивающих защищенную цифровизацию Академии, включая организацию проработки вопросов информационной безопасности при реализации цифровых решений;

– организация апробации и применения новых методов защиты информации Академии от современных угроз;

– обеспечение применения безопасных цифровых технологий при внедрении отечественных разработок и развитии собственного программного обеспечения Академии;

– обеспечение соответствия информационной безопасности и защиты информации требованиям законодательства и иным нормативно-правовым актам Российской Федерации;

– исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

– предотвращение несанкционированного доступа к информационным активам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

– предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

– предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

– недопущение использования информационных активов и содержащейся в них информации не по назначению;

– исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

– недопущение распространения с использованием информационных активов противоправной информации;

– обеспечение возможности восстановления доступа авторизованных пользователей к информационным активам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

– обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

5. Принципы защиты информации и информационной безопасности

Деятельность Академии в области защиты информации и информационной безопасности осуществляется с соблюдением следующих основных принципов:

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

2) Централизация функций управления – возможность принятия управленческих решений в области защиты информации и информационной безопасности Академии за счет оперативного мониторинга (ИТ-пространства Академии и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности, защиты информации; осуществления централизованного управления стратегическими инициативами по защите информации и информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности и защите информации; создания и развития централизованных решений в области защиты информации и информационной безопасности.

3) Управление рисками – включает мониторинг, анализ и оценку появляющихся актуальных и будущих рисков и угроз информационной безопасности с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Академии.

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

5) Импортозамещение – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счет ориентирования на отечественные решения, средства и сервисы при осуществлении Политики Академии.

6) Ресурсное обеспечение – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной безопасности и защиты информации Академии, поддержание требуемой организационной структуры.

7) Законность и соответствие – деятельность по обеспечению защиты информации и информационной безопасности Академии основывается на выполнении требований нормативных правовых актов Российской Федерации.

8) Повышение культуры информационной безопасности – декларирует необходимость не только информировать всех работников Академии, абитуриентов, обучающихся, контрагентов и других лиц, использующих ИТ-активы Академии, о требованиях к защите информации и информационной безопасности, но и развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами Академии.

9) Развитие компетенций и профессионализма – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по защите информации, информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей.

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

11) 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 Академии 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;

12) осуществляется регулярная оценка уровня зрелости процессов защиты информации в соответствии с установленными нормативно-правовыми актами Российской Федерации требованиями о защите информации, в том числе в соответствии с п.32 Требований. Информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги) – означает, что предлагаемые и оказываемые Академии или в интересах Академии ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

13) Совместимость – подразумевает подбор компонентов для обеспечения защиты информации, 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 Академии.

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

15) Адекватность и обоснованность решений – принимаемые в Академии меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Академии.

16) 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 Академии, его контрагентам, работникам, обучающимся, абитуриентам.

17) 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 информационных системах (ИС) и в автоматизированных системах управления (АСУ), ограничение прав доступа, в зависимости от уровня согласованных полномочий. Любому работнику Академии доступ к информационным ресурсам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами. При необходимости должен осуществляться организационный и программно-аппаратный контроль конфликта полномочий.

18) 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.

6. Объекты обеспечения информационной безопасности

В рамках обеспечения защиты информации и информационной безопасности объектами защиты в Академии являются объекты доступа и информация, обрабатываемая в информационных системах Академии.

К объектам доступа относятся:

– автоматизированные рабочие места, средства обработки информации и мобильные технические средства;

– информационные системы, системы хранения данных, программное обеспечение и отдельные технические решения;

– автоматизированные системы;

– информационно-технологическая и виртуальная инфраструктура;

– информационно-телекоммуникационные сети и системы связи, каналы связи и сетевые интерфейсы (в том числе беспроводные);

– информационные сервисы (ИТ-услуги, оказываемые Академии или в интересах Академии);

– виртуальная инфраструктура (гипервизоры, виртуальные машины, контейнеры);

– съемные машинные носители информации (флеш-накопители, внешние диски);

– периферийные устройства (принтеры, сканеры, многофункциональные устройства);

– решения по цифровизации Процессов Академии.

Категории защищаемой информации:

1) Информация ограниченного доступа (персональные данные, служебная тайна, коммерческая тайна, иная информация, доступ к которой ограничен федеральными законами).

2) Общедоступная информация, нарушение целостности или доступности которой может привести к нарушению образовательных, научных, финансово-хозяйственных и иных уставных процессов Академии.

3) Метаданные и техническая информация об информационных системах, средствах вычислительной техники, сетях и пользователях, разглашение которой может способствовать реализации угроз безопасности информации.

7. Ответственность за нарушения в области информационной безопасности

Работники Академии должны выполнять требования и правила защиты информации и информационной безопасности при работе с информацией, в том числе касающейся самих работников, абитуриентов, обучающихся, контрагентов, а также при работе с ИТ-активами Академии и контрагентов.

Требования распорядительных документов и правил обеспечения защиты информации и информационной безопасности обязательны для всех без исключения работников Академии и должны учитываться во взаимоотношениях с абитуриентами, обучающимися и контрагентами.

Руководство Академии возлагает ответственность на уполномоченных руководителей структурных подразделений Академии за организацию деятельности по обеспечению защиты информации и информационной безопасности как неотъемлемой составляющей Процессов Академии; за своевременную идентификацию значимых ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Академии, абитуриентам, обучающимся и контрагентам, использующим ИТ-активы Академии, и контроль за их выполнением.

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

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

Работники контрагентов, абитуриенты, обучающиеся, использующие ИТ-активы Академии, а также предоставленную Академией информацию, несут ответственность в соответствии с договорными отношениями с Академией, а также в соответствии с законодательством Российской Федерации. Факт несоблюдения контрагентом требований Политики Академии является основанием для расторжения договора в одностороннем порядке.

8. Ликвидация последствий нарушения Политики Академии

В случае обнаружения работником, абитуриентом, обучающимся, контрагентом Академии факта нарушения информационной безопасности или осуществления несанкционированного доступа к защищаемым информационным ресурсам Академии они обязаны незамедлительно об этом проинформировать работников структурного подразделения Академии, ответственного за обеспечение защиты информации, информационной безопасности.

Работник структурного подразделения Академии, на которого возложена обязанность обеспечить защиту информации, информационную безопасность, используя полученные от работников, абитуриентов, обучающихся, контрагентов Академии данные, а также данные полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации

в информационных системах и ресурсах Академии, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

Порядок действий при обнаружении инцидента, включая оповещение, локализацию, ликвидацию последствий и восстановление функционирования информационных систем, определяется Порядком реагирования на инциденты информационной безопасности, разрабатываемым в соответствии с пунктом 36 Требований.

9. Доведение и распространение Политики Академии

Академия доводит Политику Академии до абитуриентов, работников, обучающихся и своих контрагентов и взаимодействует с ними с учетом Политики Академии.

Ознакомление с Политикой является обязательным для всех работников Академии при приёме на работу (под подпись), а также для контрагентов – до предоставления доступа к информационным системам Академии.

Настоящая Политика принимается Ученым советом Академии и утверждается приказом ректора Академии. Политика вступает в силу со дня издания приказа о ее утверждении или в срок, указанный в этом приказе.

Изменения и дополнения в настоящую Политику Академии принимаются и утверждаются в том же порядке, в котором принята и утверждена настоящая Политика Академии.

Перечень защищаемых информационных систем и компонентов информационно-телекоммуникационной инфраструктуры определен в Приложении №1 к Политике Академии. Его актуализация проводится при вводе в эксплуатацию новых информационных систем или выводе из эксплуатации существующих, но не реже одного раза в год.