Министерство культуры Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Академия хорового искусства имени В.С. Попова»

ПРИКАЗ

06 февраля 2025 г. Москва №16-25-ОД

Об организации работы по
информационной безопасности

В соответствии с Указом Президента РФ от 01.05.2022 №250, Федеральными законами: от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями), от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2023) и Уставом федерального государственного бюджетного образовательного учреждения высшего образования «Академия хорового искусства имени В.С. Попова» (далее – Академия),

П Р И К А З Ы В А Ю:

1. Признать утратившим силу приказ от 22 мая 2023 г. № 49-23-ОД «О назначении ответственного за информационную безопасность».
2. Утвердить Положение об информационной безопасности (приложение № 1).
3. Утвердить ответственных за информационную безопасность в Академии (приложение № 2).
4. Системному администратору Мацкову Н.А. разместить приказ на сайте Академии.
5. Приказ вступает в силу с момента подписания.
6. Контроль выполнения приказа оставляю за собой.

И.о. ректора,
профессор **А.В. Соловьёв**

Приложение №1
к приказу
от 06.02 2025 г. №16-25-ОД
«Об организации работы по информационной безопасности»

Положение об информационной безопасности

1. Общая информация

1. Настоящее Положение об информационной безопасности определяет цели и принципы обеспечения информационной безопасности[1] в федеральном государственном бюджетном учреждении высшего образования «Академия хорового искусства имени В.С. Попова»[2].

2. Основными принципами информационной безопасности в Академии являются:

- конфиденциальность – меры по предотвращению несанкционированного разглашения информации;
- целостность – обеспечение точности и надёжности данных и исключение их некорректного изменения случайно либо умышленно;
- доступность – защита способности информационной системы Академии делать информацию полностью или (при необходимости) частично доступной, когда они нужны пользователю (или в определённое время).

3. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность — в случае внесения в данные исключительно авторизованных изменений, доступность — при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

4. Целями обеспечения информационной безопасности являются минимизация ущерба от угроз информационной безопасности и улучшение деловой репутации и корпоративной культуры Академии. Руководители подразделений Академии должны обеспечить регулярный контроль за соблюдением Положения. Кроме того, необходимо организовывать периодическую проверку соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководству.

5. Ответственность за соблюдение требований информационной безопасности несёт каждый сотрудник и лицо, работающее в Академии по договору гражданско-правового характера[3], в части, касающейся автоматизированного рабочего места.

---

[1] Далее – Положение.
[2] Далее – Академия.
[3] Далее – сотрудники, если не оговорено иное.

6. На лиц, работающих в Академии по договорам гражданско-правового характера, в том числе прикомандированных, настоящее Положение распространяются в случае, если это предусмотрено условиями договора.

2. Контроль доступа к информационным системам

2.1. Общие положения

7. Все работы в пределах Академии выполняются в соответствии с официальными должностными обязанностями только на автоматизированных рабочих местах (компьютерах)[4], разрешенных к использованию в Академии.

8. Руководители структурных подразделений должны на регулярной основе (не реже одного раза в квартал) проверять и при наличии необходимости пересматривать права доступа подчинённых сотрудников и других пользователей к информационным ресурсам, доступ к которым был ранее им санкционирован.

9. Для обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему нужно производить только с использованием уникального имени пользователя и пароля. Сотрудники должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

10. Во время работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 10 минут.

11. При необходимости покинуть служебное помещение, в котором находится компьютер, сотрудник обязан заблокировать его с целью исключения доступа к информационным ресурсам Академии посторонних лиц.

2.2. Доступ третьих лиц к системам Академии

12. Сотрудник обязан немедленно уведомить своего непосредственного руководителя обо всех случаях предоставления доступа третьим лицам к ресурсам внутренней информационной системы Академии. Доступ третьих лиц к информационным системам Академии возможен только по служебной необходимости с санкции руководства Академии.

2.3. Удаленный доступ

13. Сотрудникам Академии может быть предоставлен удаленный доступ к сетевым ресурсам Академии, в соответствии с правами во внутренней информационной системе.

14. Сотрудникам, работающим в дистанционном и частично дистанционном режиме вне места дислокации Академии с использованием

---

[4] Далее – компьютер.

компьютера, не принадлежащего Академии, в режиме удалённого доступа, запрещается копировать данные на накопитель информации, являющийся его неотъемлемой частью.

15. Сотрудники Академии и иные лица, имеющие право удаленного доступа к информационной системе Академии, обязаны соблюдать требование об исключении одновременного подключения их компьютера к сети Академии и иным не принадлежащим Академии сетям.

16. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.4. Доступ к сети Интернет

17. Доступ сотрудников Академии к сети Интернет в Академии обеспечивается только в служебных целях и не может использоваться для противоправной деятельности.

18. Рекомендованные правила:

- сотрудникам разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение сайтов в сети Интернет, содержащих пропаганду национальной и расовой ненависти (нетерпимости), написание и рассылка комментариев по поводу различия/превосходства полов, дискредитирующих заявлений или иных материалов с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности и иную противоправную информацию экстремистского характера;
- сотрудники не должны использовать сеть Интернет (т.н. «облачные» хранилища информации, удалённые серверы, личные электронные почтовые ящики) для хранения данных Академии;
- работа сотрудников с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Академии в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Академии;
- сотрудники перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Академии для всех лиц, не являющихся сотрудниками Академии, включая членов семьи сотрудников.

19. Системные администраторы Академии имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

3. Защита оборудования

20. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Академии.

3.1. Аппаратное обеспечение

21. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться в службу технической поддержки Академии.

22. При записи какой-либо информации на носитель для передачи его контрагентам необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

23. Мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства, не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию об Академии и её сотрудниках.

3.2. Программное обеспечение

24. Все программное обеспечение, установленное на предоставленном Академией компьютерном оборудовании, является собственностью Академии и должно использоваться исключительно в служебных целях.

25. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника.

26. Сотрудникам Академии запрещается:

- блокировать антивирусное программное обеспечение;
- устанавливать антивирусное программное обеспечение, отличное от установленного специалистами Академии;
- изменять настройки и конфигурацию установленного специалистами Академии антивирусного программного обеспечения.

4. Правила пользования электронной почтой

27. Содержание электронных почтовых сообщений должно строго соответствовать стандартам в области этики служебного поведения работников организаций, подведомственных Министерству культуры Российской Федерации.

28. Сотрудникам запрещается направлять по электронной почте без использования систем шифрования вне информационной системы Академии конфиденциальную информацию Академии.

Запрещается использование личных электронных почтовых ящиков для осуществления какого-либо из видов служебной деятельности.

29. Недопустимые действия и случаи использования электронной почты Академии:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям Академии сообщений/писем, не связанных со служебной деятельностью;
- подписка на рассылку и рассылка рекламных материалов;
- участие в дискуссиях в социальных сетях и иные действия, не связанные с исполнением служебных обязанностей, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, не относящихся к исполнению служебных обязанностей.

5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

30. Все пользователи информационных систем Академии должны быть осведомлены о своей обязанности сообщать руководству Академии об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности для нанесения материального или репутационного ущерба интересам Академии и её сотрудников.

31. При выявлении наличия вирусных (содержащих вредоносные программные коды) программ в программном обеспечении Академии или на компьютерах и иных носителях информации, подключаемых к компьютерам, сразу после их обнаружения сотрудник обязан:

- проинформировать системного администратора Академии;
- не пользоваться и не выключать компьютер, на котором обнаружено вредоносное программное обеспечение;
- не подсоединять вышеуказанный компьютер к информационной сети Академии до тех пор, пока на нем не будет произведено удаление обнаруженного вредоносного программного обеспечения и полное антивирусное сканирование компьютера и информационной системы Академии системными администраторами.

Приложение №2
к приказу от 06.02 2025 г. № 16-25-ОД
«Об организации работы
по информационной безопасности»

Ответственные
за информационную безопасность

Ответственность	ФИО ответственного	Должность	Подпись
1. Контроль содержания информации, предоставляемой заведующими кафедр, руководителями структурных подразделений, ответственными лицами из числа профессорско-преподавательского состава Академии: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале и информационных табло Академии; - для заполнения отчетов и мониторингов.	Красногорова Ольга Альбертовна	Первый проректор-проректор по учебно-воспитательной работе и развитию	
1. Контроль содержания информации, предоставляемой специалистами отдела подготовки кадров высшей квалификации: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале и информационных табло Академии; - для заполнения отчетов и мониторингов.	Ефимова Наталья Ильинична	Проректор по научной работе	
1. Контроль содержания информации, предоставляемой специалистами отдела обеспечения основной деятельности: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале и информационных табло Академии; - для заполнения отчетов и мониторингов.	Критская Ольга Валентиновна	Проректор по финансам и административно-хозяйственной работе	
1. Контроль за содержанием, организация, сбор и выставление информации на информационные ресурсы: - официальный сайт Академии (https://axu.ru/);	Кожин Николай Вячеславович	Помощник первого проректора-проректора по	

-социальная сеть «ВКонтакте»; -Телеграмм-канал и информационное табло Академии; - мониторинговые и статистические отчеты Министерств и ведомств РФ.		учебно-воспитательной работе и развитию	
1. Осуществление сбора и анализа информации по фактам нарушений информационной безопасности. 2. Проведение служебных расследований по фактам нарушений, доклад результатов ректору.	Румынин Виталий Витальевич	Помощник ректора по общим вопросам	
1. Контроль содержания информации, предоставляемой специалистами учебного отдела и концертмейстерами Академии: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале и информационных табло Академии; - для заполнения отчетов и мониторингов.	Добронравова Татьяна Дмитриевна	Начальник отдела по учебно-воспитательной работе	
1. Контроль содержания, организация, сбор и выставление информации на: - официальный сайт Академии (https://axu.ru/); - информационные ресурсы, координирующие организацию, проведение Приемной кампании Академии; - мониторинговые и статистические отчеты Министерств и ведомств РФ.	Кочетова Лариса Витальевна	Заместитель начальника отдела по учебно-воспитательной работе	
1. Контроль содержания информации, предоставляемой педагогическими работниками и сотрудниками Хорового училища имени А.В. Свешникова: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале и информационных табло Академии; - для заполнения отчетов и мониторингов.	Музылева Елена Евгеньевна	Заведующий Хоровым училищем имени А.В. Свешникова	
1. Контроль содержания информации, предоставляемой сотрудниками финансово-экономического отдела Академии: - для размещения на официальном сайте (https://axu.ru/), - для заполнения отчетов и мониторингов, связанных с финансово-экономической деятельностью Академии.	Юрикова Екатерина Николаевна	Заместитель начальника финансово-экономического отдела	

1. Контроль содержания информации, предоставляемой сотрудниками ЦНО: - для размещения на официальном сайте (https://axu.ru/), - для заполнения отчетов и мониторингов, связанных с работой ЦНО.	Суханова Татьяна Борисовна	Руководитель Центра непрерывного образования и повышения квалификации творческих и управленческих кадров в сфере культуры	
1. Контроль содержания информации, предоставляемой сотрудниками ЦП: - для размещения на официальном сайте (https://axu.ru/), видеохостинге «Rutube», социальной сети «ВКонтакте», Телеграмм-канале, информационных табло Академии и др. информационных ресурсах; - для заполнения отчетов и мониторингов, связанных с работой ЦП.	Татарицкий Петр Константинович	Руководитель Центра прототипирования «Центр современной музыки и исполнительских искусств»	
1. Контроль содержания информации, предоставляемой сотрудниками библиотеки: - для размещения на официальном сайте (https://axu.ru/); - для заполнения отчетов и мониторингов, связанных с работой библиотеки.	Реуцкая Елена Матвеевна	Заведующий библиотекой	
1. Контроль содержания, организация, сбор и выставление информации на информационные ресурсы: - официальный сайт Академии (https://axu.ru/); - мониторинговые и статистические отчеты Министерств и ведомств РФ; - в программы 1С, СБИС, Работа в России и др.	Лоткова Татьяна Эльяровна	Специалист по персоналу	
1. Контроль содержания, организация, сбор и выставление информации на информационные ресурсы: - официальный сайт Академии (https://axu.ru/); - мониторинговые и статистические отчеты Министерств и	Морозова Татьяна Васильевна	Специалист по кадровому учету обучающихся	

ведомств РФ; - в программы 1С: Предприятие, ФИС ФРДО.			
1.Установка, замена, контроль за работой электронной почты сотрудников Академии. 2.Организация, установка и контроль за удаленным доступом к сетевым информационным ресурсам Академии сотрудников, имеющим право удаленного доступа к информационным системам Академии. 3. Контроль: - за работой защищенной сети и своевременными обновлениями антивирусной защиты; - содержания всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях; - за изменениями конфигураций аппаратного и программного обеспечения, использованием компьютерного оборудования исключительно в служебных целях. 4. Управление и контроль за использованием сотрудниками Академии сетевых ресурсов и папок общего пользования. 5. Установка, настройка, подключение персональных компьютеров сотрудникам Академии. 6.Организация и информационно-безопасное техническое сопровождение работы сотрудников Академии в программах ФИС ГИА, ФИС ФРДО, 1С: Предприятие, СБИС, Работа в России, Суперсервис «Поступи в ВУЗ онлайн» и др.	Селезнев Александр Валентинович	Системный администратор	
1.Взаимодействие с сотрудниками по размещению информации на официальном сайте Академии (https://axu.ru/). 2. Поддержание сайта Академии в рабочем состоянии и контроль за его информационной безопасностью	Мацков Николай Александрович	Системный администратор	