Министерство культуры и туризма Пензенской области
Государственное бюджетное профессиональное образовательное учреждение
«Пензенский музыкальный колледж им. А.А. Архангельского»

«УТВЕРЖДЕНО»

приказом ГБПОУ «Пензенский
музыкальный колледж им.
А.А. Архангельского»
№ 99 от «28» апреля 2023 г.

ПОЛОЖЕНИЕ

об информационной безопасности в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»

Пенза, 2023 г.

1. Общие положения

1.1. Положение «Об информационной безопасности в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»», является локальным нормативным актом Государственного бюджетного профессионального образовательного учреждения «Пензенский музыкальный колледж им. А.А. Архангельского»» (далее – Колледж), устанавливает порядок доступа пользователей к информационным ресурсам Колледжа и порядок обеспечения безопасности информационных ресурсов.

1.2. Действие настоящего Положения не распространяется на:

- отношения, связанные с обеспечением доступа к персональным данным, которые регулируются Положением «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»», утв. приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» № 23 от 23.01.2023 г.;
- подготовка ответов на обращения (предложения, заявления, жалобы) граждан, которая регулируется Инструкцией по делопроизводству Государственного бюджетного профессионального образовательного учреждения «Пензенский музыкальный колледж им. А.А. Архангельского», утв. приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» № 153 от 24.10.2022 г.;
- информацию о деятельности Колледжа составляющую государственную тайну, требования по работе со сведениями, относящимися к государственной тайне, установлены нормативными правовыми актами Российской Федерации.

1.3. Настоящее Положение разработано в соответствии с:

- Трудовым кодексом Российской Федерации,
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» с изменениями и дополнениями,
- Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» с изменениями и дополнениями,
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями и дополнениями,
- Правилами размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, утв. Постановлением Правительства Российской Федерации от 20.10.2021 г. № 1802;
- постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- приказом Федеральной службы по надзору в сфере образования и науки от 14.08.2020 № 831 «Требования к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации» с изменениями и дополнениями.

1.4. К объектам информационной безопасности в Колледже относятся информационные ресурсы, содержащие:

- обязательную информацию о деятельности Колледжа;
- информацию о частной жизни работников Колледжа;
- информацию о частной жизни обучающихся Колледжа;

- конфиденциальную информацию о деятельности Колледжа, представленную в виде документированных информационных массивов и баз данных.

II. Цели и задачи обеспечения безопасности информации

2.1. Под информационной безопасностью Колледжа следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также права и обязанности работников и обучающихся Колледжа - субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

2.2. Главной целью обеспечения безопасности информационных ресурсов Колледжа, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Колледжа.

2.3. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, относящейся к информационным ресурсам Колледжа;
- предотвращение нарушений прав личности обучающихся, работников Колледжа на сохранение конфиденциальности информации об их частной жизни;
- предотвращение несанкционированных действий по блокированию информации.

2.4. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Колледжа, нарушению нормального функционирования и развития Колледжа;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- развитие и совершенствование защищенного юридически значимого документооборота;
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;
- создание механизмов управления системой информационной безопасности.

III. Меры по обеспечению информационной безопасности

3.1. Система информационной безопасности должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

3.2. Колледж обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты объектов информационной безопасности от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

Под угрозами безопасности информации понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия.

Под уровнем защищенности информации понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности информации.

3.3. Обеспечение информационной безопасности в Колледже достигается, в частности:

1) определением угроз безопасности информации в информационных системах;

2) применением организационных и технических мер по обеспечению безопасности в информационных системах, необходимых для выполнения установленных требований к защите информации;

3) учетом машинных носителей информации в Колледже;

4) обнаружением фактов несанкционированного доступа к информационным ресурсам Колледжа и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы и по реагированию на компьютерные инциденты в них;

5) восстановлением информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) контролем за принимаемыми мерами по обеспечению безопасности информации и уровня защищенности информационных систем;

7). назначением должностных лиц Колледжа, ответственных за осуществление информационной безопасности.

3.4. Колледж обязан в установленном порядке, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) информации Колледжа.

3.5. Делопроизводство в Колледже ведется на основании Инструкции по делопроизводству Государственного бюджетного профессионального образовательного учреждения «Пензенский музыкальный колледж им. А.А. Архангельского», утв. приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» № 153 от 24.10.2022 г.

Система организации делопроизводства осуществляется назначенным приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» должностным лицом, которое отвечает за:

- учет всей документации Колледжа, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрацию и учет всех входящих (исходящих) документов в специальном журнале;
- особый режим уничтожения документов Колледжа.

3.6. Перечень обязательной для предоставления информации о деятельности Колледжа устанавливается законодательными актами Российской Федерации и уполномоченными органами в запросах, инструктивных письмах и т.д.

3.7. Требования к порядку формирования структурированной информации о Колледже и требования к форматам структурированной информации и файлов, содержащих электронные копии документов, устанавливаются уполномоченным органом.

3.8. Защита персональных данных в Колледже от неправомерного их использования или утраты обеспечена Колледжем за счет его средств в порядке, установленном федеральным законом «О персональных данных» и в соответствии с Положением «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»», утв. приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» № 23 от 23.01.2023 г.

3.9. Колледж обеспечивает безопасность передаваемой информации уполномоченным органам о работниках и обучающихся Колледжа:

- в целях предупреждения угрозы их жизни и здоровью;
- в Фонд пенсионного и социального страхования Российской Федерации, в объеме, предусмотренном законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов государственной безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников, обучающихся Колледжа,
- сведения о работниках, обучающихся Колледжа (в том числе: работнике - уволенном, обучающимся Колледжа – отчисленном) могут быть предоставлены другой организации только по письменному мотивированному запросу на бланке организации.

Персональные данные работника, обучающегося Колледжа могут быть предоставлены их законным представителям, членам семьи, только с письменного разрешения самого субъекта ПД или в порядке, предусмотренном законодательством Российской Федерации, ограничиваясь только той информацией, которая необходима для выполнения указанными представителями их функций.

3.10. Контроль за подлинностью и актуальностью содержания информации о деятельности Колледжа для размещения на официальном сайте, а так же передаваемой уполномоченному органу информации несет должностное лицо, ответственное за обеспечение информационной безопасности Колледжа.

IV. Основные принципы и способы обеспечения доступа к информации о деятельности Колледжа

4.1. В соответствии с требованиями федерального законодательства Российской Федерации Колледж посредством размещения на официальном сайте в сети «Интернет» обеспечивает открытость и доступность:

1) информации:

а) о дате создания Колледжа, об учредителях образовательной организации, о представительствах и филиалах образовательной организации, о месте нахождения образовательной организации, ее представительств и филиалов (при наличии), режиме, графике работы, контактных телефонах и об адресах электронной почты;

б) о структуре и об органах управления образовательной организацией;

в) о реализуемых образовательных программах с указанием учебных предметов, курсов, дисциплин (модулей), практики, предусмотренных соответствующей образовательной программой;

г) о численности обучающихся по реализуемым образовательным программам за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов и по договорам об образовании за счет средств физических и (или) юридических лиц, о численности обучающихся, являющихся иностранными гражданами;

д) о языках образования;

е) о федеральных государственных образовательных стандартах, федеральных государственных требованиях, об образовательных стандартах;

ж) о руководителе образовательной организации, его заместителях, руководителях филиалов образовательной организации (при их наличии);

з) о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы;

з.1) о местах осуществления образовательной деятельности, сведения о которых не включаются в соответствующую запись в реестре лицензий на осуществление образовательной деятельности;

и) о материально-техническом обеспечении образовательной деятельности (о доступе к информационным системам и информационно-телекоммуникационным сетям, об электронных образовательных ресурсах, к которым обеспечивается доступ обучающихся);

к) о результатах приема по каждой профессии, специальности среднего профессионального образования (при наличии вступительных испытаний), с указанием средней суммы набранных баллов по всем вступительным испытаниям, а также о результатах перевода, восстановления и отчисления;

л) о количестве вакантных мест для приема (перевода) по каждой образовательной программе, по профессии, специальности, направлению подготовки (на места, финансируемые за счет бюджетов субъектов Российской Федерации, местных бюджетов, по договорам об образовании за счет средств физических и (или) юридических лиц);

м) о наличии и об условиях предоставления обучающимся стипендий, мер социальной поддержки;

н) о наличии общежития, количестве жилых помещений в общежитии, интернате для иногородних обучающихся, формировании платы за проживание в общежитии;

о) об объеме образовательной деятельности, финансовое обеспечение которой осуществляется за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов, по договорам об образовании за счет средств физических и (или) юридических лиц;

п) о поступлении финансовых и материальных средств и об их расходовании по итогам финансового года;

р) о трудоустройстве выпускников;

с) о лицензии на осуществление образовательной деятельности (выписке из реестра лицензий на осуществление образовательной деятельности);

2) копий документов:

а) устава Колледжа;

б) свидетельства о государственной аккредитации (с приложениями);

в) плана финансово-хозяйственной деятельности образовательной организации, утвержденного в установленном законодательством Российской Федерации порядке, или бюджетной сметы образовательной организации;
г) локальных нормативных актов, правил внутреннего распорядка обучающихся, правил внутреннего трудового распорядка, коллективного договора;

3) отчета о результатах самообследования;

4) документа о порядке оказания платных образовательных услуг, в том числе образца договора об оказании платных образовательных услуг, документа об утверждении стоимости обучения по каждой образовательной программе;

5) предписаний органов, осуществляющих государственный контроль (надзор) в сфере образования, отчетов об исполнении таких предписаний;

6) иной информации, которая размещается, опубликовывается по решению Колледжа и (или) размещение, опубликование которой являются обязательными в соответствии с законодательством Российской Федерации.

4.2. Основными принципами обеспечения доступа к информации о деятельности Колледжа являются:

- открытость и доступность информации о деятельности Колледжа, за исключением информации ограниченного доступа (государственная, коммерческая и иная охраняемая законом тайна);
- достоверность информации о деятельности Колледжа и своевременность ее предоставления;
- свобода поиска, получения, передачи и распространения открытой к доступу информации о деятельности Колледжа любым законным способом;
- соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права организаций на защиту их деловой репутации.

4.3. Доступ к информации о деятельности Колледжа обеспечивается следующими способами:

- обнародование (опубликование) Колледжем информации о своей деятельности на официальном сайте Колледжа;
- размещение Колледжем информации о своей деятельности на информационных стендах в занимаемых помещениях в СМИ;
- предоставление информации о деятельности Колледжа по запросу уполномоченных органов;
- другими способами, предусмотренными законами и (или) иными нормативными правовыми актами Российской Федерации.

4.4. Структура и содержание информации о деятельности Колледжа, размещенной на официальном сайте Колледжа, определяются Колледжем самостоятельно в соответствии с требованиями законодательства Российской Федерации.

4.5. Структура и содержание обязательной информации о деятельности Колледжа, передаваемой уполномоченному органу, определяются уполномоченным органом.

4.6. Обнародованию (опубликованию в СМИ, размещению на официальном сайте Колледжа) подлежит открытая для доступа информация о деятельности Колледжа.

Информация о деятельности Колледжа, размещенная на официальном сайте Колледжа подлежит обновлению в порядке, установленном законодательством Российской Федерации.

4.7. Ответственность за подлинность и актуальность содержания информации о деятельности Колледжа на официальном сайте, несет должностное лицо Колледжа, назначенное приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского».

V. Организация работы с информационными ресурсами и технологиями Колледжа

5.1. Использование сети «Интернет» в Колледже осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности пользователем может осуществлять доступ к ресурсам не образовательной направленности.

5.2. Использование в Колледже сети «Интернет» подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

5.3. Работники Колледжа вправе:

- размещать информацию в сети «Интернет» на интернет-ресурсах Колледжа;
- иметь учетную запись электронной почты на интернет-ресурсах Колледжа.

5.4. Работникам Колледжа запрещено размещать в сети «Интернет» и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства Российской Федерации и локальным нормативным актам Колледжа;
- не относящуюся к образовательному процессу и не связанную с деятельностью Колледжа;
- нарушающую нравственные и этические нормы, требования профессиональной этики.

5.5. Обучающиеся Колледжа вправе:

- использовать ресурсы, размещенные в сети «Интернет», в том числе интернет-ресурсы Колледжа, в порядке и на условиях, которые предусмотрены настоящим Положением.
- размещать информацию и сведения на интернет-ресурсах Колледжа.

5.6. Обучающемся запрещено:

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушает законодательство Российской Федерации;
- осуществлять любые сделки через сеть «Интернет»;
- загружать файлы на компьютер Колледжа без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

Запрет и снятие такого запрета на допуск пользователей к работе в сети «Интернет» устанавливает назначенное приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского» уполномоченное лицо.

5.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса и покинуть данный ресурс. Уполномоченное лицо обязано:

- принять сообщение пользователя;
- принять меры по отключению выхода на данный ресурс с интернет-ресурсов Колледжа;
- если обнаруженный ресурс явно нарушает законодательство Российской Федерации - сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации.

Передаваемая информация должна содержать:

- адрес интернет-ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

VI. Должностное лицо, ответственное за осуществление информационной безопасности

6.1. Должностное лицо, ответственное за осуществление информационной безопасности Колледжа (далее- уполномоченное лицо):

- назначается приказом ГБПОУ «Пензенский музыкальный колледж им. А.А. Архангельского»;
- в своей работе руководствуется законодательством Российской Федерации и настоящим Положением;

6.2. Уполномоченное лицо обязано:

- следить за соблюдением требований по парольной защите, хранить в тайне пароли, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава), в соответствии с установленными правилами (приложение №1);
- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочем месте;
- выполнять соответствующие требования инструкции по организации антивирусной защиты (приложение №2). Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день;
- выполнять соответствующие требования инструкции по обеспечению сохранности документов, дел и изданий, содержащих сведения конфиденциального характера (приложение №3);
- немедленно оповещать специалиста по защите информации в случае:
- обнаружения нарушения целостности пломб на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к оборудованию, несанкционированных изменений в конфигурации программных или аппаратных средств;
- утери индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей;
- некорректного функционирования установленных на компьютере технических средств защиты,
- обнаружения непредусмотренных отводов кабелей и подключенных устройств.

6.3. Уполномоченному лицу запрещается:

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно непредусмотренные любые программные и аппаратные средства (модемы, сотовые телефоны, цифровые фотоаппараты);
- записывать и хранить информацию на неучтенных носителях информации;

- оставлять без присмотра своё рабочее место, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- передавать кому-либо свои индивидуальные устройства идентификации (кроме специалиста по защите информации или директору Колледжа), делать неучтенные копии индивидуальных устройств идентификации (на любой другой носитель), вносить какие-либо изменения в файлы индивидуального устройства идентификации;
- оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- осуществлять попытки несанкционированного или неправомерного доступа к ресурсам, проводить или участвовать в сетевых атаках, в том числе:

1) осуществлять действия, направленные на нарушение нормального функционирования системы (компьютеров, другого оборудования или программного обеспечения);
2) устанавливать программное обеспечение, осуществляющее перехват информации, адресованной другим пользователям;
3) производить действия, направленные на получение несанкционированного или неправомерного доступа к ресурсам, в последующем использовании такого доступа, а также в несанкционированном уничтожении или модификации программного обеспечения или персональных данных;
4) осуществлять действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного или неправомерного доступа к любым системам и службам либо на нарушение целостности и работоспособности этих систем;
5) осуществлять попытки подбора паролей либо атак по словарю.

6.4. Уполномоченное лицо, виновное в нарушении норм, регулирующих порядок осуществления информационной безопасности Колледжа, несет дисциплинарную, материальную, административную или уголовную ответственность в соответствии с федеральными законами Российской Федерации.

VII. Заключительные положения

7.1. При необходимости в Положение могут быть внесены изменения и дополнения в порядке, установленном трудовым законодательством для принятия локальных нормативны актов.

7.2. Положение обязательно для размещения на официальном сайте Колледжа в информационно-телекоммуникационной сети «Интернет».

Приложение №1
к Положению «Об информационной безопасности в
Государственном бюджетном профессиональном образовательном
учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использование и прекращение действия паролей во всех информационных системах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на специалиста по защите информации Колледжа.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать латинские буквы и цифры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены о дисциплинарной ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. После использования имен и паролей некоторых работников (исполнителей) в их отсутствие, при наличии технологической необходимости в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., работники обязаны сразу же сменить свой пароль.

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться специалистом по защите информации немедленно после окончания последнего сеанса работы данного пользователя на ПК.

6. В случае компрометации личного пароля пользователя должны быть немедленно приняты меры в соответствии с п. 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Хранение работником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем сейфе.

Приложение №2
к Положению «Об информационной безопасности в
Государственном бюджетном профессиональном образовательном
учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция по организации антивирусной защиты

Общие положения

1. Настоящая инструкция определяет правила, которыми должны руководствоваться работники при организации антивирусной защиты.
2. Целью защиты является предотвращение ущерба от действий, производимых вирусами и другими вредоносными программами.

Область применения

Положения настоящей инструкции распространяются на все работы, связанные с обеспечением антивирусной защиты в Колледже, а также на всех работников, которым предоставлен доступ к информационным ресурсам Колледжа.

Правила использования средств антивирусной защиты

1. К использованию допускаются только лицензионные антивирусные средства.
2. Установка и настройка параметров средств антивирусного контроля на рабочих станциях и серверах Колледжа осуществляется специалистом по защите информации.
3. Обновление антивирусных средств должно происходить в автоматическом режиме. Допускается работа антивируса с обновлениями не старше 72 часов.
4. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться еженедельно.
5. На каждой рабочей станции и сервере в резидентном режиме должен быть запущен антивирусный монитор.
6. Обязательному антивирусному контролю подлежит любая информация, получаемая по телекоммуникационным каналам связи и на съемных носителях.
7. Устанавливаемое программное обеспечение должно быть предварительно проверено на наличие вирусов.
8. Каждый пользователь должен быть осведомлен об опасности заражения вирусами и обучен работе с антивирусным программным обеспечением.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении возлагается на специалиста по защите информации. Ответственность за проведение мероприятий антивирусного контроля в подразделении возлагается на ответственного за обеспечение безопасности информации. За нарушение положений данной инструкции работники Колледжа могут быть отстранены от доступа к информационным ресурсам Колледжа и несут ответственность в соответствии с законодательством Российской Федерации.

Приложение №3
к Положению «Об информационной безопасности в
Государственном бюджетном профессиональном образовательном
учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция
«О порядке обеспечения сохранности документов, дел и изданий, содержащих сведения конфиденциального характера»

1. Все имеющиеся документы, дела и издания, содержащие конфиденциальную информацию, должны храниться в служебных помещениях в надежно запираемых шкафах или сейфах. Помещения должны отвечать требованиям режима, обеспечивающего физическую сохранность находящейся в них документации. При необходимости шкафы, сейфы и служебные помещения могут опечатываться личными металлическими номерными печатями работников. Дубликаты ключей от шкафов и сейфов, в которых хранятся конфиденциальные документы, сдаются в опечатанных конвертах уполномоченному лицу.

2. Конфиденциальные документы хранятся (в шкафах или сейфах) отдельно от неконфиденциальных документов. При совместном хранении конфиденциальные документы группируются в папках (скоросшивателях), чтобы отделить их от неконфиденциальных документов.

3. Запрещается оставлять на рабочих местах без присмотра или в незапертых шкафах (сейфах) конфиденциальные документы в течение рабочего дня или по его окончании.

4. Доступ посторонних лиц в помещения, предназначенные для работы с конфиденциальной информацией, по возможности, ограничивается. Для работы с посетителями используются отдельные места для переговоров.

При нахождении в помещении, где проводится работа с конфиденциальными документами, посторонних лиц (в том числе сотрудников, не допущенных к данным сведениям), документы должны убираться в шкаф или сейф, чтобы исключить случайное ознакомление посторонних с конфиденциальными документами.

5. С конфиденциальными документами разрешается работать только в служебных помещениях. Для работы вне служебных помещений необходимо разрешение руководителя структурного подразделения.

6. Конфиденциальные документы могут передаваться для работы и временного хранения другим работникам, допущенным к этим документам, только под расписку. Передача подобных документов, дел, изданий в другие подразделения на постоянное хранение осуществляется через директора Колледжа.

7. Уничтожение конфиденциальных документов проводится в порядке, установленном локальным нормативным актом Колледжа.

ЛИСТ ознакомления

с Положением «Об информационной безопасности в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»» ознакомлены:

№ п/п	Фамилия, имя, отчество	Подпись и дата