Российская Федерация
Министерство культуры Краснодарского края
Государственное бюджетное научно-творческое учреждение культуры Краснодарского края
КУБАНСКИЙ КАЗАЧИЙ ХОР
ОСНОВАН В 1811 ГОДУ
ИНН 2309066787 / КПП 230901001, 350063, Россия, г. Краснодар, ул. Красная, 5 тел.: (861) 255-75-03, 262-35-99, факс: 268-31-47, www.kkx.ru

ПРИКАЗ

«08» 10 2019 г. № 323 -ОД

г. Краснодар

Об утверждении Положения о парольной защите в государственном бюджетном научно-творческом учреждении культуры Краснодарского края «Кубанский казачий хор»

В целях исключения несанкционированного доступа к информационным ресурсам в целях исключения утечки конфиденциальной информации, а также несанкционированной модификации или уничтожения данных, п р и к а з ы в а ю :

1. Утвердить Положение о парольной защите в государственном бюджетном научно-творческом учреждении культуры Краснодарского края «Кубанский казачий хор» (далее - Положение) приложение №1 к настоящему приказу.

2. Назначить администратором системы парольной защиты учреждения инженера-программиста по защите персональных данных отдела компьютерного обеспечения и сетевых технологий И.А. Протасова.

3. Начальнику отдела маркетинга и рекламы О.В. Ушаковой обеспечить размещение на официальном сайте учреждения Правил обработки персональных данных в ГБНТУК КК «Кубанский казачий хор».

4. Руководителям планово-экономического отдела (Мамий Р.Б.), отдела кадрового и документационного обеспечения (Подолян О.В.), бухгалтерии (Мамчур Т.М.), юридического отдела (Хорошавин Д.С.), гастрольно-концертного отдела (Чадаева Э.Ю.), начальнику жилищного комплекса «Театральный» (Саковский А.М.), главному инженеру (Кулага Е.П.) обеспечить контроль за исполнением подчинёнными положений вышеуказанных Правил.

5. Контроль за исполнение настоящего приказа возложить на начальника отдела компьютерного обеспечения и сетевых технологий С.А. Касянчука.

Первый заместитель
генерального директора А.Е. Арефьев

Приложение к приказу ГБНТУК КК
«Кубанский казачий хор» от ___.___.2019г.
№ _____ – ОД

Государственное бюджетное
научно-творческое учреждение культуры
Краснодарского края
«Кубанский казачий хор»

УТВЕРЖДАЮ
генеральный директор
ГБНТУК КК «Кубанский
казачий хор»
_____ В.Г. Захарченко
«___» _____ 2019 г.

Положение
о парольной защите в государственном бюджетном научно-творческом учреждении культуры Краснодарского края «Кубанский казачий хор»

I. Общие положения

1.1. Положение о парольной защите в государственном бюджетном научно-творческом учреждении культуры Краснодарского края «Кубанский казачий хор» (далее - Положение) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах государственного бюджетного научно-творческого учреждения культуры Краснодарского края «Кубанский казачий хор» (далее - учреждение), а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями.

1.2. Аутентификация легальных субъектов доступа осуществляется с помощью парольной защиты, персонального кода доступа, электронных ключей и других программно-технических средств разграничения доступа пользователей. Способ аутентификации легальных пользователей определяется в соответствии с уровнем конфиденциальности информации.

1.3. Активное сетевое оборудование (маршрутизаторы и сетевые принтеры) не должно допускать возможности несанкционированной переконфигурации, в связи с чем, каждое активное сетевое устройство должно быть защищено уникальным паролем.

1.4. Операционные системы серверов, компьютерной сети должны настраиваться таким образом, чтобы блокировать вход в сеть (на 5-15 минут) после троекратной ошибки в наборе пароля.

1.5. Если позволяют возможности операционной системы необходимо запретить выбор пользователем простых паролей средствами операционной системы.

1.6. Положение определяет требования к парольной защите информационных систем и распространяется на всех пользователей и информационные системы учреждения, использующих парольную защиту.

II. Термины и определения

ИС – любая информационная система, для работы с которой необходима аутентификация пользователя.

Пароль – секретный набор символов, используемый для аутентификации пользователя.

Пользователи – администраторы ИС и работники учреждения или сторонней организации, которым предоставлен доступ к ИС учреждания, а также корпоративный доступ к ресурсам сети Интернет.

Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

Аутентификация – установление того, что пользователь является именно тем, кем он себя объявил путем проверки предъявленного пароля.

Инициализационный пароль – пароль, выдаваемый пользователю для первоначального входа в ИС.

Информационный актив – данные, информация, сведения, обрабатываемые и хранимые в учреждении с помощью ИС.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности рабочего процесса, минимизации рисков потери.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Принцип минимальных привилегий - принцип, согласно которому «каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

III. Порядок формирования паролей

3.1. В качестве парольной информации следует выбирать последовательность букв верхнего и нижнего регистра, цифр и служебных символов длиной не менее восьми знаков.

3.2. Категорически запрещается использование в качестве пароля легко угадываемых последовательностей символов типа: названия учетной записи, номеров телефонов, имен своих и родственников, последовательно расположенные на стандартной клавиатуре символы, табельный номер и т.п. Запрещается также использование в качестве паролей слов распространенных мировых языков, независимо от раскладки клавиатуры, в которой оно набирается (например, слово МАШИНА – VFIBYF).

3.3. В пароле, кроме буквенных последовательностей, обязательно должны присутствовать цифры и специальные символы (@, #, $, &, *, % и т.п.).

3.4. Если позволяют возможности системы аутентификации рекомендуется наряду с английскими буквами использовать буквы русского алфавита (с переключением набора символов на клавиатуре).

3.5. Рекомендуется в виде пароля выбирать последовательности типа “X0Posh#1”, “!1рыБ@lkA” или “Def*en$6”

3.6. При смене пароля пользователям запрещается использовать ранее использованные пароли.

3.7. Выбор одноразовых паролей осуществляется по тем же требованиям.

3.8. Длина пароля администратора информационного ресурса должна быть не менее 11 символов. Пароль не должен содержать, ни какой логики. Например “k$iu^sd26Fx”.

3.9. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом указанных требований.

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

При введении нового пользователя администратор информационного ресурса может назначить для него инициализационный пароль, персональный код либо другую уникальную информацию для доступа к информационным ресурсам компьютерной сети. Пользователь обязан заменить инициализационный пароль – личным при первом же подключении к информационному ресурсу компьютерной сети.

3.10. В случае, когда формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников, ответственных за организацию работы ИС в учреждении. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3.11. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

IV. Период действия паролей и кодов доступа пользователей

4.1. Периодичность смены пароля задается администратором информационного ресурса централизованно, для всех пользователей.

4.2. Период действия паролей для сетевых компьютеров не должен превышать 3 месяцев, для не сетевых компьютеров – 6 месяцев.

4.3. При сообщении компьютерной системы об окончании срока действия личного пароля пользователь обязан заменить его на новый, ранее не применявшийся.

4.4. Период действия паролей для входа в АРМ автоматизированной системы не должен превышать 3 месяцев.

4.5. Персональные коды, электронные ключи и другие средства разграничения доступа меняются по требованию пользователя не реже установленного периода.

4.6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу ИС после окончания последнего сеанса работы данного Пользователя с системой.

4.7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду

работы были предоставлены полномочия по управлению парольной защитой ИС.

V. Конфиденциальность паролей и кодов доступа

5.1. Информация о паролях пользователей является конфиденциальной информацией.

5.2. Операционные системы, серверов и рабочих станций должны быть настроены таким образом, чтобы исключить возможность ознакомления пользователей и администраторов с действующими и истекшими паролями.

5.3. Информационные системы должны быть настроены таким образом, чтобы исключить возможность ознакомления пользователей и администраторов с действующими и истекшими паролями.

5.4. Информация о персональных кодах, электронных ключах и других средств доступа пользователей к информационному ресурсу является конфиденциальной информацией и разглашению не подлежит, должна содержать защиту от доступа посторонних лиц.

5.5. Хранение Пользователем своих паролей на бумажном носителе допускается в местах исключающих возможность ознакомления с ним посторонних лиц и других сотрудников.

VI. Правила работы и обязанности сотрудников по использованию и сохранению в тайне личного пароля

6.1. Пароли могут быть выданы только владельцу. В случае нарушения опечатки на конверте или его утери, пароли считается скомпрометированными и подлежит немедленной смене.

6.2. Если пользователь уверен в правильности ввода названия учетной записи и пароля, но ему не удается войти в систему, пользователь обязан незамедлительно сообщить об этом администратору информационного ресурса для получения нового одноразового пароля.

6.3. Если пользователь заметит несанкционированное появление, изменение или удаление информации, он должен немедленно изменить свой пароль и сообщить об обнаруженных изменениях начальнику отдела, администратору информационного ресурса и (или) администратору информационной безопасности.

6.4. Набор личного пароля следует проводить, в отсутствии лиц, которые потенциально могут увидеть процесс набора.

6.5. При оставлении рабочего места необходимо завершить открытую пользовательскую сессию либо использовать функцию «временной блокировки» рабочей станции.

6.6. Для предотвращения случайного оставления рабочего места с открытой пользовательской сессией рекомендуется использовать Screen Saver с автоматической блокировкой, включающийся автоматически, если компьютер не используется в течение определенного времени.

6.7. Запрещается:

- передача личного пароля сослуживцам или руководителям подразделений (-я);
- запись личного пароля доступа на материальные носители (напр. бумагу, дискеты) в открытом виде;

- вход в компьютерную сеть и информационную систему с использованием чужих идентификаторов и паролей доступа;

- оставлять без присмотра рабочее место с открытой пользовательской сессией.

6.8. В случае подозрения о компрометации пароля, сотрудники обязаны произвести экстренную замену личного пароля и незамедлительно поставить об этом в известность администратора информационной безопасности для исключения возможности утечки информации.

6.9. Любые действия сотрудников и посторонних лиц нарушающие требования настоящего Положения, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.

VII. Ответственность

7.1. Пользователи:

- исполняют требования настоящего Положения и несут ответственность за его нарушение.

- информируют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего Положения.

7.2. Администратор парольной защиты:

- принимает обращения пользователей по вопросам парольной защиты (блокировка учетных записей, нарушение положения и др.), ведет их учет.

- организует консультации пользователей по вопросам использования парольной защиты.

- контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.

- отвечает за безопасное хранение паролей встроенных административных учетных записей.

Лист согласования
к приказу от _____ № _____

«Положение о парольной защите в государственном бюджетном научно-творческом учреждении культуры Краснодарского края «Кубанский казачий хор»

Согласовано:
Заместитель генерального
директора
_____ В.Н. Лютый «____» _____ 2019г.

Начальник юридического отдела
_____ Д.С. Хорошавин «03» 10 2019г.

И.о.главного инженера
_____ Б.К. Ашинова «03» 10 2019г.