УТВЕРЖДАЮ
ДИРЕКТОР ГБУК
«Балаклавский Дворец культуры»

_____М.Ю.Ткачева

Парольная политика в Государственном бюджетном учреждении культуры города Севастополя «Балаклавский Дворец культуры» (ГБУК «БДК»)

Севастополь 2022

Оглавление

Термины и определения

ИБ - информационная безопасность

Информационный актив - информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Государственного бюджетного учреждения культуры города Севастополя «Балаклавский Дворец культуры», находящаяся в распоряжении Государственного бюджетного учреждения культуры города Севастополя «Балаклавский Дворец культуры» и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

НРД - нерегламентированные действия в рамках предоставленных полномочий;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

АРМ - автоматизированное рабочее место;

ИСПДн - информационная система персональных данных

1. Общие положения

1.1. Назначением Парольной политики является формулирование общих требований к организации парольной защиты информации при работе в Государственном бюджетном учреждении культуры города Севастополя «Балаклавский Дворец культуры» (далее ГБУК «БДК») и повышение осведомленности персонала (работников) в области информационной безопасности.

1.2. Требования настоящей политики распространяются на всех пользователей ГБУК «БДК», включая площадки, и все компоненты ИТ-инфраструктуры ГБУК «БДК».

1.3 Пароли являются важнейшим аспектом информационной безопасности и обеспечивают защиту учетных записей пользователей. Неправильно выбранный пароль повышает потенциальный риск несанкционированного доступа к информационным системам общества. Все работники ГБУК «БДК» (а также представители подрядной организации и третьей стороны) несут ответственность за невыполнение требований настоящей политики.

1.4. Работники ГБУК «БДК», допустившие нарушение настоящей политики, могут быть привлечены к дисциплинарной ответственности в порядке, установленном трудовым законодательством Российской Федерации.

2. Цели и задачи парольной политики

Цель парольной политики - предотвращение НСД и/или НРД к информационным активам ГБУК «БДК».

Настоящая политика определяет требования к организации парольной защиты, а также устанавливает единые правила парольной защиты для:

- средств вычислительной техники;
- приложений и активного сетевого оборудования;
- программного обеспечения;
- ИСПДн,
- других защищаемых информационных активов ГБУК «БДК» (файлы данных и т.п.).

В ГБУК «БДК» должны быть определены роли и назначены ответственные лица в соответствии с «Разрешительной системы доступа (матрица доступа) к информационным (программным) ресурсам ГБУК «БДК».

В основе Политики лежит структурный подход к парольной защите, при котором должны обеспечиваться следующие условия:

- пароль является средством защиты АРМ, серверов, приложений, активного сетевого оборудования, ПО и сведений конфиденциального характера от НСД и представляет собой числовую и символьную последовательность, состоящую из определенного количества знаков (символов).
- пароль эффективен как средство защиты только при правильном его использовании.

3. **Регламент парольной защиты**

Пароли могут быть индивидуальными и коллективными. Индивидуальный пароль принадлежит только одному пользователю и применяется для разграничения доступа в многопользовательских системах, а также для доступа к ресурсам индивидуального пользования. Коллективный пароль принадлежит нескольким пользователям, объединяемым в соответствующую группу, и применяется в многопользовательских системах для доступа к общим ресурсам и в системах с одним технически возможным паролем, если требуется обеспечить доступ к системе нескольких пользователей.

Использование индивидуальных и коллективных паролей строго контролируется инженером по защите информации ГБУК «БДК».

Пароли должны держаться в тайне, то есть не должны сообщаться другим людям, в открытом виде не должны содержаться в текстах программ или файлах и записываться на любые виды носителей информации.

Пользователь должен принять все меры для того, чтобы исключить возможность компрометации [1] принадлежащего ему пароля.

Пользователь несет персональную ответственность за сохранность своего пароля в конфиденциальности.

Пароли технологического доступа (стандартные пароли фирм производителей, предназначенные для доступа к системным ресурсам, серверам, АРМ и активному сетевому оборудованию) должны быть изменены или заблокированы.

При выборе пароля следует руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы нижнего и верхнего регистров, цифры и специальные символы (@#$& * % и т.п.);
- запрещается использовать в качестве паролей номера телефонов, имена, фамилии, даты дней рождений и иные подобные сочетания;
- при смене пароля новое значение не должно совпадать ни с одним из 5 последних ранее используемых паролей.

Для обеспечения доступа пользователю к информационным ресурсам, руководитель подразделения направляет заявку установленной формы на имя директора ГБУК «БДК» (Приложение № 1) с указанием вида доступа исполнителя к тем или иным подсистемам (сетевые ресурсы, базы и т.д.).

---

[1] Компрометация — событие, приведшее к несанкционированному получению пароля посторонними лицами.

Пароли должны периодически меняться. При отсутствии иных локальных нормативных актов ГБУК «БДК», регламентирующих периодичность смены пароля в конкретном случае, пароль должен меняться не реже одного раза в три месяца. При компрометации пароля он должен меняться немедленно. По факту компрометации пароля необходимо немедленно направить служебную записку инженеру по защите информации ГБУК «БДК».

4. Требования политики

4.1. Пароли системных учетных записей (администратора домена, локального администратора, root и т.д.) должны соответствовать следующим требованиям:

- изменяться не реже, чем 1 раз в квартал;
- содержать не менее восьми символов;
- не являться словом, которое используется в словарях (русских или иностранных);
- содержать сочетания букв верхнего и нижнего регистров, цифры и спецсимволы;
- храниться в базе данных в зашифрованном виде, доступ к которой ограничен;
- учитываться в журнале учета паролей (Приложение № 2). Журнал учета паролей является документом строгой отчетности, оформляется как документ «для служебного пользования», хранится в опечатываемом металлическом хранилище ГБУК «БДК».

4.2. Пароли администраторов приложений и активного сетевого оборудования должны соответствовать следующим требованиям:

- изменяться не реже, чем 1 раз в полгода;
- содержать не менее восьми символов;
- не являться словом, которое используется в словарях (русских или иностранных);
- содержать сочетания букв верхнего и нижнего регистров, цифры и спецсимволы; _ храниться в базе данных в зашифрованном виде, доступ к которой ограничен;
- быть уникальными для каждого оборудования и приложения.

4.3. Пароли учетных записей пользователей должны соответствовать следующим требованиям:

- изменяться не реже, чем 1 раз в полгода;
- содержать не менее восьми символов;
- не являться словом, которое содержится в словарях (русских или иностранных);
- храниться в зашифрованном виде в базе данных, доступ к которой ограничен.

4.4. Пароль учетной записи пользователя, имеющего административные привилегии, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.

4.5. Запрещена передача паролей пользователям по телефону, при помощи почтовых сообщений либо иным другим открытым способом через Интернет.

4.6. Новый пароль пользователя не должен совпадать ни с одним из пяти последних применявшихся им паролей.

4.7. При пяти неправильных попытках ввода пароля учетная запись пользователя блокируется на 1 час.

4.8. Если пользователь считает, что его пароль стал известен кому-либо, он должен сменить пароль и сообщить о компрометации инженеру по защите информации ГБУК «БДК» по телефонам: 63-73-79 или на адрес электронной почты: balaclava@mail.ru.

4.9. Запрещено сообщать свой пароль кому-либо, включая руководителей, секретарей, коллег, родственников, системных администраторов, специалистов службы технической поддержки, а также записывать и хранить его в легкодоступном месте.

4.10. Если кто-либо требует от пользователя сообщить его пароль, то пользователю необходимо сослаться на настоящую политику или направить требующего к инженеру по защите информации ГБУК «БДК».

4.11. Инженером по защите информации ГБУК «БДК» могут проводиться проверки паролей пользователей на стойкость к подбору или взлому. Если во время таких мероприятий пароль будет подобран или взломан, учетная запись будет заблокирована. Для разблокировки и смены пароля пользователю необходимо обратиться к Директору ГБУК «БДК».

4.12. Для некоторых АРМ, ПО и информации могут предъявляться специальные требования по длине, содержанию, частоте и порядку смены паролей. Эти требования устанавливаются в иных локальных нормативных актах ГБУК «БДК».

5. Ответственность

Ответственность за соблюдение требований данной Политики в ГБУК «БДК» возлагается на его руководителя.

Контроль за правильным использованием паролей осуществляют руководители подразделений, инженер по защите информации ГБУК «БДК».

6. Заключительные положения

Настоящая Политика вступает в силу с момента ее утверждения Директором ГБУК «БДК».

Настоящую политику необходимо пересматривать и при необходимости вносить в нее изменения один раз в три года или в случае существенных изменений в ИТ-инфраструктуре или организационной структуре ГБУК «БДК», а также в случае инцидентов информационной безопасности, способных повлиять на процесс, описанный в Политике.

Все изменения в настоящую Политику вносятся приказом Директора ГБУК «БДК».

Настоящая Политика действует до момента его отмены или принятия нового документа.

Если при изменении законодательства Российской Федерации отдельные статьи Политики вступают в противоречие с ним, то эти статьи утрачивают свою юридическую силу, и до момента внесения изменений в документ, работники ГБУК «БДК» руководствуются действующим законодательством Российской Федерации, при этом факт прекращения действия одного или нескольких пунктов не влияет на действие Политики в целом.

Приложение № 1
к Парольной политике в ГБУК «Балаклавский Дворец Культуры»

Форма заявки на обеспечение
доступа к информационным
ресурсам

_____

наименование подразделения

Кому: Директору ГБУК «БДК»

От кого: _____

«__»_____20__ г.

От Руководителя подразделения
Ф.И.О.

Тема: О предоставлении доступа

ЗАЯВКА

Прошу обеспечить доступ работника (должность, Ф.И.О.) к следующим информационным ресурсам:

_____

_____

_____

Руководитель подразделения Ф.И.О.

Согласовано:

Директор ГБУК «БДК» Ф.И.О.

Исполнитель: Ф.И.О.

Инженер по защите
информации

Приложение № 2
к Парольной политике в ГБУК «Балаклавский Дворец Культуры»

Журнал
учета назначаемых паролей

№ п/п	Дата	Назначение пароля (числовая и символьная последовательность	Наименование ресурса	Примечание

Инженер по защите информации

Ф.И.О.