Приложение 9

УТВЕРЖДЕНО
Приказом ГАОУ ВО МИОО
от 25.10.2017 № 406/ОД

ПАРОЛЬНАЯ ПОЛИТИКА В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ «МОСКОВСКИЙ ИНСТИТУТ ОТКРЫТОГО ОБРАЗОВАНИЯ»

Москва, 2017 г.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящая Парольная политика в Государственном автономном образовательном учреждении высшего образования города Москвы «Московский институт открытого образования» (далее – Политика) является внутренним нормативным документом Государственного автономного образовательного учреждения высшего образования города Москвы «Московский институт открытого образования» (далее – Институт) и не подлежит представлению другим сторонам без согласования с ректором Института.

1.2. Настоящий документ определяет требования к парольной защите ресурсов Института, включая требования к паролям, порядок их генерации, изменения и использования.

1.3. Цель настоящей Политики – минимизация риска несанкционированного доступа к информационным системам Института за счет использования слабостей в организации парольной защиты.

1.4. Настоящая Политика распространяется на все элементы информационных систем и структурные подразделения Института, а также на третьих лиц, использующих и/или обслуживающих информационные системы Института. При внедрении новых и при модернизации существующих элементов информационных систем, должны учитываться все положения настоящей Политики.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие термины, определения и сокращения:

ИБ – информационная безопасность.

Институт – Государственное автономное образовательное учреждение высшего образования города Москвы «Московский институт открытого образования»

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов, а также иная информация, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также информационные системы и их элементы, служащие для обработки документов (информации).

Офицер ИБ - работник Института, назначенный приказом ректора Института на роль ответственного за обеспечение информационной безопасности в Институте, в том числе безопасности персональных данных.

СУБД – система управления базами данных.

ФИО - фамилия, имя, отчество.

3. ОСНОВНЫЕ ПОЛОЖЕНИЯ

3.1. Все учетные записи (включая системные, служебные и учетные записи пользователей и администраторов) в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к BIOS и к управлению персональными межсетевыми экранами и антивирусным

программным обеспечением) должны быть защищены стойкими методами аутентификации.

3.2. Пароль является средством защиты от несанкционированного доступа к информации или к средствам ее обработки, хранения, передачи, и эффективен только при правильном его использовании.

3.3. В информационных системах, в базах данных, на серверах, в других системах и устройствах Институт должны быть задействованы (при наличии технической возможности) механизмы, реализующие принудительное исполнение пользователями требований настоящей Политики:

- ограничения на минимальную длину пароля;
- периода действия пароля;
- запрета на повтор недавно используемых паролей;
- проверки паролей на сложность;
- блокирование учетной записи при превышении установленного числа попыток неправильного ввода пароля;
- обязательную смена пароля, установленного пользователю администратором системы, при первой регистрации пользователя в системе.

4. ГЕНЕРАЦИЯ ПАРОЛЕЙ

4.1. При предоставлении пользователю прав доступа в информационной системе администратор задает ему первоначальный пароль, уникальный для каждого пользователя.

4.2. Первоначальный пароль передается пользователю лично в руки либо сообщается устно. Запрещается передавать пользователю пароль в открытом виде по электронной почте и другим открытым каналам связи.

4.3. При первом входе в систему пользователь обязан сменить первоначальный пароль, заданный администратором.

4.4. Пароли всех внутренних пользователей (сотрудников Института) и администраторов, используемые в информационных системах Института, должны отвечать следующим требованиям сложности:

1) длина пароля должна быть не менее 8 символов;
2) пароль должен содержать символы, по крайней мере, из трех приведенных групп:
   - буквы латинского алфавита в верхнем регистре (A-Z),
   - буквы латинского алфавита в нижнем регистре (a-z),
   - цифры (0-9),
   - специальные символы и знаки пунктуации (например, !@#$%^&*(),.?);
3) период действия пароля не более 90 дней.

4.5. Пароли для внешних пользователей обучающих веб-систем, являющихся внешними преподавателями, не имеющими доступа к конфиденциальной информации, или же обучающимися, должны отвечать следующему требованию сложности: длина пароля должна быть не менее 6 символов.

4.6. Пароли технологических учетных записей, используемых в Институте, должны отвечать следующим требованиям сложности:

1) длина пароля технологических учетных записей должна быть не менее 14 знаков;

2) пароли технологических учетных записей должны содержать в себе символы из всех следующих групп:

- буквы латинского алфавита в верхнем регистре (A-Z),
- буквы латинского алфавита в нижнем регистре (a-z),
- цифры (0-9),
- специальные символы и знаки пунктуации (например, !@#$%^&*(),.?).

4.7. При выборе нового пароля запрещается циклическое использование старых паролей: новый пароль не должен совпадать ни с одним из последних 5 (пяти) ранее использовавшихся паролей.

4.8. При выборе паролей не должна использоваться какая-либо «система»: новый пароль не должен быть прогнозируем на основе знаний о предыдущих паролях, датах их смены и т.п.

4.9. Пользователь должен выбирать трудно подбираемые пароли. При выборе пароля запрещается:

- использовать в пароле подряд идущие в алфавите или раскладке клавиатуры символы (например, «QWErtyu», «qazxswEDC», «zyxwVUTS» и пр.);
- использовать в пароле осмысленные слова, сленговые выражения или общеупотребительные сокращения, имена собственные (названия, имена и фамилии), в том числе набранные на регистре другого языка или преобразованные транслитерацией (например, «grapefruit», «Churchill», «admin», «cbcntvf» (система), «svetofor» и пр.);
- включать в пароль последовательности из трех и более повторяющихся символов (например, «qqqAAA123», «ad1111C», «ZZZZaaaa1» и пр.);
- включать в пароль ассоциированную с пользователем или информационной системой информацию: ФИО пользователя или его ближайших родственников, марку автомобиля, идентификатор пользователя в информационной системе, название информационной системы или сервера и т.д. (например, «dmitry666»).

5. ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ

5.1. Пароль должен быть известен только его владельцу. Запрещается сообщать пароль кому бы то ни было, в том числе администраторам систем и работникам управления информатизации.

5.2. Работники обязаны обеспечить конфиденциальность своих паролей. Запрещается разглашать и передавать свои пароли другим работникам, хранить пароли в открытом доступе, а также сохранять пароли в открытом (не защищенном) виде на магнитных носителях. При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами.

5.3. При покидании рабочего места более чем на 2 (две) минуты пользователь обязан заблокировать свой компьютер.

5.4. В случае компрометации (факт ознакомления с паролем лица, не являющегося его владельцем) пароля или подозрении на компрометацию пользователь обязан уведомить об этом офицера ИБ Института и незамедлительно сменить свой пароль.

5.5. Запрещается включение паролей в автоматизированный процесс регистрации (например, с использованием хранимых макрокоманд или функциональных клавиш) без применения дополнительных мер защиты.

5.6. При использовании встроенных учетных записей на системных компонентах (серверы, СУБД, сетевое оборудование, средства виртуализации, прикладное программное обеспечение, средства защиты информации) запрещено использовать пароли, установленные производителем по умолчанию.

5.7. Все пароли должны быть приведены к нечитаемому виду при передаче и хранении на всех системных компонентах с помощью алгоритмов надежной криптографии.

5.8. После 5 (пяти) неудачных попыток аутентификации пользователя (за исключением внешних пользователей обучающих веб-систем) его учетная запись должна автоматически блокироваться. При этом разблокировка учетной записи должна выполняться:

– либо автоматически, но не ранее чем через 45 (сорок пять) минут после ее блокировки;

– либо вручную системным администратором.

5.9. При более чем 15-минутной неактивности пользователя, должна выполняться автоматическая блокировка сеанса. Возможность продолжения работы пользователя с системой должна быть обеспечена после повторного прохождения аутентификации (повторный запрос пароля пользователя).

6. ИЗМЕНЕНИЕ ПАРОЛЕЙ

6.1. Срок действия паролей пользователей и администраторов систем не должен превышать 90 дней. Срок действия паролей внешних пользователей обучающих веб-систем не ограничен.

6.2. Внеплановая смена пароля пользователя системы осуществляется в случае выявления факта компрометации пароля. Смена пароля пользователя должна производиться немедленно после выявления факта компрометации пароля.

6.3. Внеплановая смена пароля администратора системы осуществляется в случае выявления факта компрометации пароля, а также в случае прекращения полномочий администратора системы (увольнение, переход на другую работу внутри Института и другие обстоятельства). Смена пароля администратора системы должна производиться немедленно после выявления факта компрометации пароля, или прекращения полномочий администратора.

6.4. Перед сменой пароля пользователь должен пройти аутентификацию.

6.5. В случае утраты пароля пользователем пароль может быть заново назначен администратором системы с соблюдением следующих требований:

– смена пароля пользователя администратором осуществляется только на основании письменной заявки, согласованной руководителем пользователя и офицером ИБ;

– пароль, заданный администратором, передается лично пользователю;

– при первом входе в систему пользователь обязан сменить пароль, заданный администратором;

– отработанные заявки на изменение паролей с пометкой администратора о выполнении хранятся не менее 1 (одного) года.

6.6. Срок действия паролей технологических учетных записей не должен превышать одного года. При этом в целях повышения уровня доступности информационных систем Института не рекомендуется устанавливать технические/программные ограничения срока действия паролей технологических учетных записей.

6.7. Администраторы информационных систем Института, владельцы технологических учетных записей обязаны осуществлять смену пароля от управляемых ими учетных записей при поступлении задания через автоматизированную систему постановки задач. Каждая смена пароля технологической учетной записи должна быть зафиксирована в автоматизированной системе постановки задач.

7. ОТВЕТСТВЕННОСТЬ

7.1. Ответственность за обеспечение технической поддержки положений настоящей Политики возлагается на администраторов информационных систем.

7.2. Контроль за соблюдением требований настоящей Политики возлагается на офицера ИБ Института.

7.3. Работники Института, использующие информационные ресурсы Института, несут персональную ответственность за соблюдение настоящей Политики, а также за все действия, произведенные в информационных системах Института с использованием их учетной записи и пароля.