АНО «НИИ микрохирургии»

ПОЛОЖЕНИЕ
о парольной защите при обработке персональных данных и иной конфиденциальной информации

УТВЕРЖДАЮ
Байтингер В.Ф.
Президент АНО «НИИ микрохирургии»
_____ _____
(подпись) (расшифровка подписи)
"12" января 2017 г.

1. Общие положения

1.1. Для обеспечения конфиденциальности, целостности и доступности информационных активов АНО «НИИ микрохирургии (далее – Организация) использует наряду с другими средствами парольную защиту. Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

1.2. Положение определяет требования Организации к парольной защите информационных систем.

1.3. Положение распространяется на всех пользователей и информационные системы (далее – ИС) Организации, использующих парольную защиту.

2. Термины и определения

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 Обществе с помощью ИС.

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

Компрометация пароля – известность пароля или принципа его формирования посторонним лицам.

Пароль – секретный набор символов, используемый для аутентификации пользователя.

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

СТП – служба технической поддержки, подразделения ИТ.

УИС – Управление информационных систем Организации.

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

3. Положения

3.1. Каждая учетная запись должна быть защищена паролем.

3.2. Для доступа в ИС пользователю выдается инициализационный пароль, который он обязан сменить при первом входе в ИС.

3.3. Пользователь обязан использовать различные пароли для каждой учетной записи.

3.4. Учетная запись пользователя блокируется после трех неудачных попыток ввода пароля. Разблокировка учетной записи возможна только после обращения пользователя в СТП.

3.5. Пользователь обязан менять пароли для доступа к корпоративным ИС не реже чем раз в 180 календарных дней.

3.6. При выборе пароля пользователь обязан соблюдать следующие требования:

3.6.1. Минимальная длина пароля пользователя составляет не менее 8-ми символов.

3.6.2. Пароль должен состоять из комбинации цифр, букв латинского алфавита верхнего и нижнего регистра.

3.6.3. Новый пароль не должен повторять пять использованных ранее паролей.

3.7. Пользователь обязан применять адекватные меры по защите своих паролей:

3.7.1. Запоминать свои пароли или хранить их таким образом, чтобы они были недоступны другим лицам.

3.7.2. Не передавать свои пароли никому ни под каким предлогом, включая специалистов ИТ, своего руководителя, коллег, родственников или знакомых.

3.7.3. При использовании пароля (например, его вводе) принять необходимые меры, исключающие возможность его компрометации (например, исключить возможность подглядывания вводимого пароля).

3.8. Пользователю запрещено применять пароли, используемые им при аутентификации в ИС Организации, для доступа в не принадлежащие Организации ИС (например, на веб-сайтах сети Интернет и др.).

3.9. В случае компрометации или подозрения на компрометацию пароля, пользователь обязан информировать об этом СТП и немедленно сменить пароль.

3.10. Пароли встроенных административных учетных записей (например, "root" в ОС UNIX, "Administrator" в MS Windows AD и т.п.) основных ИС, а также пароль локального администратора рабочих станций филиала должны храниться в защищенном месте в опечатанном конверте в несгораемом сейфе. Доступ к этим паролям возможен только с санкции руководителя ИТ-подразделения филиала, или Исполнительной дирекции.

3.11. Учетные записи сотрудников, имеющих членство в группах администраторов, должны иметь пароль, отличный от всех других паролей данного пользователя.

3.12. Специалистам ИТ запрещено хранить пароли пользователей в любом виде, например, в открытом или в виде хеш-функций, а также размещать пароли на ресурсах общего доступа, или пересылать их по электронной почте, за исключением пересылки пользователю инициализированного пароля.

3.13. При использовании SNMP community strings не должны быть значениями по умолчанию и должны отличаться от паролей, используемых для аутентификации в интерактивном режиме.

3.14. Смена паролей административных учетных записей, используемых на серверах и маршрутизирующем оборудовании, а также пароля локального администратора рабочих станций филиала обязательно производится в следующих случаях:

3.14.1. Компрометация либо подозрение на компрометацию паролей.

3.14.2. Увольнение из Организации лиц, которым в связи с производственной необходимостью были известны пароли.

3.14.3. Расторжение договора с подрядной организацией, сотрудникам которой выдавались пароли для выполнения работ на оборудовании Организации.

3.15. При наступлении случаев, описанных в п.3.14, создается новый пароль и опечатывается новый конверт.

3.16. ИС Организации должны иметь механизмы проверки паролей на соответствие требованиям положения.

3.17. За нарушение требований настоящего Положения на работника может быть наложено дисциплинарное или административное взыскание.

4. Роли и ответственность

4.1. Пользователи:

4.1.1. Исполняют требования положения и несут ответственность за ее нарушение.

4.1.2. Информируют СТП обо всех ставших им известных случаях нарушения настоящего положения.

4.2. СТП:

4.2.1. Принимает обращения пользователей по вопросам парольной защиты (например, блокировка учетных записей, компрометация пароля, нарушение положения и др.), ведет их учет.

4.2.2. Консультирует пользователей по вопросам использования парольной защиты.

4.2.3. Выдает пользователям инициализационные пароли для входа в ИС.

4.2.4. Отвечает за безопасное хранение паролей встроенных административных учетных записей.

4.2.5. Производит разблокировку учетных записей пользователей.

5. Исключения

Все исключения из Положения должны быть согласованы в письменном виде с УИС.