МИНИСТЕРСТВО ЭНЕРГЕТИКИ И ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА КИРОВСКОЙ ОБЛАСТИ

ПРИКАЗ

15.06.2023 № 65

г. Киров

Об утверждении некоторых инструкций в министерстве энергетики и жилищно-коммунального хозяйства Кировской области

В целях обеспечения защиты персональных данных в министерстве энергетики и жилищно-коммунального хозяйства Кировской области, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по организации парольной защиты в министерстве энергетики и жилищно-коммунального хозяйства Кировской области согласно приложению № 1.

2. Утвердить Инструкцию по антивирусной защите министерства энергетики и жилищно-коммунального хозяйства Кировской области согласно приложению № 2.

3. Утвердить Инструкцию по заполнению Журнала контроля соблюдения условий эксплуатации и работоспособности криптографической защиты информации в министерстве энергетики и жилищно-коммунального хозяйства Кировской области согласно приложению № 3.

4. Контроль за выполнением приказа оставляю за собой.

И.о. министра
энергетики и жилищно-
коммунального хозяйства
Кировской области А.В. Журавлев

Приложение № 1

УТВЕРЖДЕНА

приказом и.о. министра
энергетики и жилищно-
коммунального хозяйства
Кировской области
от 15.06.2023 № 65

ИНСТРУКЦИЯ
по организации парольной защиты в министерстве энергетики и жилищно-коммунального хозяйства Кировской области

Настоящая Инструкция по организации парольной защиты в министерстве энергетики и жилищно-коммунального хозяйства Кировской области (далее – Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей, в том числе удаление учетных записей пользователей информационных систем, а также контроль за действиями пользователей и обслуживающего персонала при работе с применением механизмов парольной аутентификации в министерстве энергетики и жилищно-коммунального хозяйства Кировской области (далее – министерство).

1. Особенности организации парольной защиты

1.1. Организационное и техническое обеспечение процессов, связанных с разграничением полномочий, присвоением идентификаторов и паролей и решением других вопросов парольной политики, а также повседневный и периодический контроль за действиями пользователей и обслуживающего персонала при работе с паролями возлагается на администратора информационной безопасности (далее – Администратор ИБ) в части организации доступа к общесистемному и прикладному программному обеспечению, а также к средствам защиты информации.

1.2. При осуществлении ответственным за организацию парольной защиты лицами (Администратор ИБ) процедур оформления и разграничения прав доступа к общесистемному, прикладному программному обеспечению и средствам защиты информации каждому пользователю централизованно назначается идентификатор и пароль, соответствующий следующим требованиям:

- при формировании логинов используется ГОСТ 7.79-2000 (ИСО 9-95) «Правила транслитерации кириллического письма латинским алфавитом» (Система Б) для перевода кириллических символов в символы латинского алфавита (пример: IvanovVA);

- длина пароля должна быть не менее 6 символов с обязательным присутствием среди них цифр, а также букв верхнего и нижнего регистра;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), общепринятые термины и сокращения (user, passw и т.д.), повторяющиеся комбинации нескольких символов, а также комбинации символов, набираемых на клавиатуре в закономерном порядке (12345, qwerty, и т.д.);

- пароль не должен являться установленным «по умолчанию» производителями программного, программно-аппаратного обеспечения;

- допускается применение специальных программных средств для генерации «стойких» значений паролей.

1.3. Первичный пароль пользователя устанавливается Администратором ИБ с учетом требований настоящей Инструкции. Пользователи обязаны в течение 24 часов с момента предоставления доступа сменить первичный пароль на постоянный с учетом требований настоящей Инструкции.

1.4. Для каждого постоянного пароля устанавливается срок его действия, который составляет 180 дней. По истечении указанного срока действия пользователь обязан осуществить смену пароля на новый.

1.5. Внеплановая смена пароля пользователя должна производиться в случае подозрения его компрометации в обязательном порядке. В случае подозрения на компрометацию пароля пользователю необходимо в кратчайшие сроки обратиться к Администратору ИБ.

1.6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий служащих, работников министерства, деятельность которых была связана непосредственно с организацией парольной защиты.

1.7. Удаление учетной записи пользователя с его идентификационной и аутентификационной информацией производится Администратором ИБ в случае прекращения полномочий данного пользователя в связи с расторжением служебного контракта и увольнения сразу же после окончания последнего сеанса работы пользователя на рабочем месте.

1.8. Учетные записи пользователей могут быть заблокированы Администратором ИБ на определенный период (отпуск, командировка, ограничение полномочий и др.) на основании служебной записки руководства. Снятие блокировки с такой учетной записи производится также на основании служебной записки руководства.

2. Обеспечение конфиденциальности паролей

2.1. Пользователи обязаны соблюдать требования настоящей Инструкции, а также необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

2.2. Пользователям запрещено:

– сообщать свой пароль кому-либо, включая других работников и руководителей, по телефону, по электронной почте или какими-либо иными средствами, а также сообщать сведения о применяемой системе защиты конфиденциальной информации;

– хранить пароль в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к нему доступ;

– записывать пароль и оставлять эти записи в местах, к которым могут получить доступ неуполномоченные лица;

– принимать какие-либо действия по получению (раскрытию) паролей других пользователей.

2.3. Если вышестоящее должностное лицо требует от пользователя раскрытия его пароля, то пользователю следует отказаться от предоставления таких сведений, сославшись на настоящую инструкцию, и предложить обратиться данному должностному лицу за разъяснениями к Администратору ИБ.

3. Ответственность

3.1. Ответственность за осуществление общего контроля выполнения требований настоящей Инструкции возлагается на Администратора ИБ.

3.2. Ответственность за доведение требований настоящей Инструкции до служащих министерства, а также контроль за их соблюдением возлагается на ответственного за организацию обработки конфиденциальной информации, в том числе персональных данных.

3.3. Ответственность за выполнение требований настоящей Инструкции возлагается на Администратора ИБ и всех служащих министерства, чья трудовая деятельность связана с доступом к информационным ресурсам.

3.4. В случае несоблюдения требований настоящей Инструкции указанные лица могут быть привлечены к дисциплинарной или иной предусмотренной законодательством РФ ответственности.

Приложение № 2

УТВЕРЖДЕНА

приказом и.о. министра
энергетики и жилищно-
коммунального хозяйства
Кировской области
от 15.06.2023 № 65

ИНСТРУКЦИЯ
по антивирусной защите в министерстве энергетики и жилищно-коммунального хозяйства Кировской области

Настоящая Инструкция по антивирусной защите в министерстве энергетики и жилищно-коммунального хозяйства Кировской области предназначена (далее – Инструкция) для пользователей и администраторов, хранящих и обрабатывающих конфиденциальную информацию на автоматизированных рабочих местах (далее – АРМ) и серверах министерства энергетики и жилищно-коммунального хозяйства Кировской области.

1. В целях обеспечения антивирусной защиты на АРМ пользователей и серверы устанавливается антивирусное программное обеспечение.

2. Ответственность за поддержание установленного в настоящей Инструкции возлагается на Администратора безопасности конфиденциальной информации.

3. К применению на АРМ пользователей и серверах допускаются лицензионные сертифицированные антивирусные средства.

4. На АРМ пользователей запрещается установка программного обеспечения, не предусмотренного технологическим процессом обработки информации.

5. Пользователи АРМ при работе со сменными носителями информации обязаны перед началом работы осуществить проверку носителя информации на предмет отсутствия компьютерных вирусов.

6. Администратор безопасности конфиденциальной информации осуществляет периодическое обновление антивирусных средств и контроль их работоспособности.

7. Администратор безопасности конфиденциальной информации проводит периодическое тестирование всего установленного программного обеспечения и данных на дисках АРМ и серверах на предмет отсутствия компьютерных вирусов.

8. При обнаружении компьютерного вируса, лечение которого не возможно установленными антивирусными средствами, пользователь обязан немедленно поставить в известность Администратора безопасности конфиденциальной информации и прекратить какие-либо действия на АРМ.

9. Администратор безопасности конфиденциальной информации проводит в случае необходимости лечение зараженных файлов посредством средств сканирования антивирусной программы.

10. В случае обнаружения на сменном носителе информации нового вируса, не поддающегося лечению, Администратор безопасности обязан запретить использование данного сменного носителя информации.

11. В случае обнаружения на жестком диске АРМ, сервера не поддающегося лечению вируса, Администратор безопасности конфиденциальной информации обязан поставить в известность лицо, ответственное за эксплуатацию АРМ, сервера, запретить работу на АРМ, сервере и в возможно короткие сроки произвести восстановление работоспособности АРМ, сервера.

12. Пользователи АРМ и администраторы серверов должны быть ознакомлены с настоящей Инструкцией.

Приложение № 3

УТВЕРЖДЕНА

приказом и.о. министра
энергетики и жилищно-
коммунального хозяйства
Кировской области
от 15.06.2023 № 65

ИНСТРУКЦИЯ
по заполнению Журнала контроля соблюдения условий эксплуатации и работоспособности криптографической защиты информации в министерстве энергетики и жилищно-коммунального хозяйства Кировской области

1. Для обеспечения и поддержания эффективности защиты информации с использованием средств криптографической защиты информации (далее – СКЗИ) в министерстве энергетики и жилищно-коммунального хозяйства Кировской области (далее –министерство) проводится контроль соблюдения условий эксплуатации и работоспособности СКЗИ в министерстве.

2. Контроль за соблюдением условий эксплуатации может осуществляться:

- как обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ, а также как собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
- лицензиатом;
- Федеральной службой безопасности Российской Федерации.

3. Контроль может быть первичным, плановым и внеплановым. Первичный контроль проводится при вводе СКЗИ в эксплуатацию. Плановый контроль осуществляется с установленной периодичностью, но не реже 1 раза в год. Внеплановый контроль осуществляется в случае установления фактов нарушения в министерстве условий эксплуатации или работоспособности СКЗИ.

4. По результатам контроля проверяющим оформляется Протокол проверки. С протоколом проверки должен быть ознакомлен министр энергетики и жилищно-коммунального хозяйства Кировской области.

5. Сведения о контроле заносятся проверяющим в Журнал контроля соблюдения условий эксплуатации и работоспособности криптографической защиты информации в министерстве энергетики и жилищно-коммунального хозяйства Кировской области (далее – Журнал). Если при контроле обнаружены недостатки, то указываются также замечания по результатам

контроля. На каждое замечание назначается лицо, ответственное за его устранение, а также срок устранения. По результатам работы над замечанием в Журнале делается запись о статусе устранения замечания, которая заверяется подписью Администратора СКЗИ.

6. Министерство обязано принять меры по устранению вскрытых недостатков и выполнению рекомендаций Лицензиата по результатам контроля.

7. Если в ходе контроля выявлены серьезные нарушения в эксплуатации СКЗИ, из-за чего становится реальной утечка конфиденциальной информации, Лицензиат вправе дать указание о прекращении использования СКЗИ до устранения причин выявленных нарушений.

8. Назначение полей Журнала:

«1» - Порядковый номер контроля

«2» - Вид контроля. Может принимать значения: первичный, плановый, внеплановый

«3» - Дата контроля

«4» - ФИО контролирующего

«5» -Замечания по результатам контроля и подпись контролирующего

«6» - отметка об устранении замечаний, дата и подпись Администратора СКЗИ.

8. Все листы Журнала должны быть пронумерованы. Журнал должен быть прошнурован, оформлен всеми подписями на титульном листе и скреплен печатью.

№ п/п	Вид контроля (плановый/ внеплановый)	Дата	ФИО контролирующего	Замечания по результатам контроля, подпись контролирующего	Дата устранения замечания, подпись Администратора СКЗИ
1	*2*	*3*	*4*	*5*	*6*