РЕГИОНАЛЬНАЯ ЭНЕРГЕТИЧЕСКАЯ КОМИССИЯ ОМСКОЙ ОБЛАСТИ

П Р И К А З

7 марта 2023 года № 3-П

г. Омск

О создании автоматизированной системы для обработки информации ограниченного доступа

В целях выполнения нормативных требований по обработке информации ограниченного доступа, не содержащей сведения, составляющих государственную тайну (для служебного пользования) (далее - Информация) приказываю:

1. Для обработки Информации создать автоматизированную систему «РЭК» Региональной энергетической комиссии Омской области (далее - АС «РЭК»).

2. Разместить АС «РЭК» в здании по адресу: 644099, г. Омск, ул. Красногвардейская дом 42.

3. Начальнику отдела информационного обеспечения Калиманову Я.М. организовать подготовку организационно-распорядительной документации и аттестацию АС «РЭК» в соответствии с действующими нормативными документами ФСТЭК России в срок до 1 мая 2023 года.

4. Приказ довести до сотрудников Региональной энергетической комиссии по Омской области.

5. Утвердить инструкцию администратора безопасности объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 1 к настоящему приказу.

6. Утвердить инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации объекта информатизации АС «РЭК» согласно приложению № 2 к настоящему приказу.

7. Утвердить инструкцию ответственного за эксплуатацию объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 3 к настоящему приказу.

8. Утвердить инструкцию по организации парольной защиты объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 4 к настоящему приказу.

9. Утвердить инструкцию по проведению антивирусного контроля объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 5 к настоящему приказу.

10. Утвердить инструкцию о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в объект информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 6 к настоящему приказу.

11. Утвердить инструкцию пользователя объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области по обеспечению безопасности обработки информации при возникновении внештатных ситуаций согласно приложению № 7 к настоящему приказу.

12. Утвердить инструкцию пользователя объекта информатизации АС «РЭК» Региональной энергетической комиссии Омской области согласно приложению № 8 к настоящему приказу.

13. Контроль за исполнением настоящего приказа возложить на заместителя председателя Меньшикова А.Ю.

Председатель
Региональной энергетической
комиссии Омской области Д.А. Русских

Приложение № 1
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
администратора безопасности
объекта информатизации автоматизированная система «РЭК» Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет функции, права и обязанности администратора безопасности автоматизированной системы «РЭК» (далее – АС) Региональной энергетической комиссии Омской области (далее – РЭК) по вопросам обеспечения информационной безопасности при обработке информации, содержащей сведения, составляющие государственную тайну.

1.2. Администратор безопасности назначается из числа сотрудников организации и обеспечивает правильность использования и нормальное функционирование установленных систем и средств защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД).

1.3. Настоящая Инструкция является дополнением к действующим руководящим и нормативным документам ФСБ России, ФСТЭК России, Правительства Российской Федерации и Министерства связи и массовых коммуникаций Российской Федерации по вопросам защиты информации, содержащей сведения, составляющие государственную тайну, и не исключает обязательного выполнения их требований.

2. ОСНОВНЫЕ ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Контроль и выполнение требований, действующих нормативных и руководящих документов по вопросам защиты информации, содержащей сведения, составляющие государственную тайну, при проведении работ на автоматизированной системе.

2.2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом на ПЭВМ:

- реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтерам и т.д.);
- ввод описаний пользователей ПЭВМ в информационную базу установленной на ПЭВМ СЗИ от несанкционированного доступа (НСД);
- своевременное удаление описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе на ПЭВМ лиц.

2.3. Контроль доступа к работе на ПЭВМ, в соответствии со списком сотрудников, допущенных к работе на ПЭВМ, контроль соблюдения пользователями требований нормативных и руководящих документов.

2.4. Контроль за проведением смены паролей для доступа пользователями ПЭВМ.

2.5. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на ПЭВМ:

- введение в базу данных установленной на ПЭВМ СЗИ от НСД описания событий, подлежащих регистрации в системном журнале;
- регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременное информирование председателя РЭК или лица, исполняющего его обязанности, о несанкционированных действиях персонала и проведение расследования попыток НСД;

2.6. Сопровождение подсистемы обеспечения целостности информации на ПЭВМ:

- периодическое тестирование функций установленной на ПЭВМ СЗИ от НСД, особенно при изменении программной среды и полномочий пользователей;
- восстановление программной среды, программных средств и настроек СЗИ при сбоях;
- ведение копии программных средств СЗИ от НСД и контроль их работоспособности;
- поддержание установленного порядка и правил антивирусной защиты информации на ПЭВМ;
- периодическое обновление антивирусных средств (баз данных), установленных на ПЭВМ, контроль соблюдения пользователями порядка и правил проведение антивирусного тестирования ПЭВМ.

2.7. Контроль наличия и целостность пломб (печатей, специальных знаков) на корпусе ПЭВМ и устройств.

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

1) Требовать от пользователей АС и обслуживающего персонала объекта информатизации соблюдения установленных правил обработки информации и выполнения требований руководящих и нормативно-методических документов по защите информации.

2) Обращаться к председателю РЭК или лицу, исполняющему его обязанности, с требованием о прекращении доступа пользователя к работам в АС в случае грубых нарушений требований руководящих и нормативно-методических документов по защите информации, порядка и правил обработки информации, или нарушения функционирования средств и систем защиты информации.

3) Требовать объяснительных документов и назначения служебного расследования в отношении пользователя АС и обслуживающего персонала объекта информатизации по фактам нарушения безопасности информации и НСД к защищаемой информации.

4) Требовать от пользователей прекращения обработки информации на АС в случае:

- нарушения установленного порядка работ,

- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСБ России или ФСТЭК России,

- получения информации о возможном проведении технической разведки в отношении АС.

5) Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа.

4. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности обязан:

1) Обеспечивать правильное функционирование и поддерживать работоспособность средств и систем защиты информации от несанкционированного доступа в пределах, возложенных на него функций.

2) Проводить инструктаж пользователей по правилам работы на ПЭВМ с установленными СЗИ от НСД.

3) В случае отказа средств и систем защиты информации принимать меры по их восстановлению.

4) Докладывать председателю РЭК или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к конфиденциальной информации, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности на объекте информатизации АС.

5) Вносить изменения в документацию на АС в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД.

6) Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учет и принимать меры к их устранению.

7) Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать соответствующему должностному лицу.

8) Вести учет машинных носителей информации.

9) Проводить работу по выявлению использования пользователями не учтенных машинных носителей информации.

10) Проводить работы по восстановлению данных, модифицированных или уничтоженных вследствие НСД к ним.

11) Не допускать на объекте установку программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

12) Осуществлять периодическое обновление антивирусных пакетов и контроль их работоспособности.

13) Проводить на постоянной основе мониторинг информационной безопасности и антивирусного контроля.

5. ПОРЯДОК ПРОВЕДЕНИЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АНТИВИРУСНОГО КОНТРОЛЯ ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

5.1. Мониторинг аппаратного обеспечения.

Мониторинг работоспособности аппаратных компонент автоматизированной системы, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

5.2. Мониторинг парольной защиты.

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 2 месяцев);
- минимальное количество символов в пароле – восемь;
- в пароле не должны использоваться общеизвестные слова и словосочетания;
- пароли не должны повторять друг друга;
- периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

5.3. Мониторинг целостности.

Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов с резервных копий при несовпадении контрольных сумм.

5.4. Мониторинг попыток несанкционированного доступа.

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

5.5. Мониторинг производительности.

Мониторинг производительности автоматизированной системы, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления

попыток несанкционированного доступа, повлекших существенное уменьшение производительности системы.

5.6. Системный аудит.

1) Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

2) Обзоры безопасности проводятся с целью проверки соответствия текущего состояния системы, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну, тому уровню безопасности, который удовлетворяет требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку для проверки.

3) Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

4) Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

5) Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

6) Внесение изменений в системное программное обеспечение осуществляется администратором безопасности, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; анализ претензий в случае, если это изменение причинило вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

5.7. Антивирусный контроль.

1) Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

- утилиты для обнаружения и анализа новых вирусов.

2) К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные ФСТЭК России средства антивирусной защиты.

3) При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

4) Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, осуществляется администратором безопасности в соответствии с руководствами по установке приобретенных средств защиты.

5) Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором безопасности на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения АС должна быть выполнена антивирусная проверка.

6) Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

7) Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

8) Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

9) Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки

(изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

10) На серверах систем, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

11) На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

12) Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

13) Необходимо проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов требуется выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

5.8. Анализ инцидентов.

1) Если существует подозрение или получено сообщение о том, что информационная система подвергается атаке или уже была скомпрометирована, то необходимо установить:

- факт попытки НСД;
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

2) Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

3) При анализе системных журналов необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия «суперпользователя» или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

4) В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

5) Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

6) В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

6. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации, которые влекут за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации объекта информатизации автоматизированной системы «РЭК» Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция о порядке резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) определяет действия, связанные с функционированием объекта информатизации (ОИ) автоматизированной системы «РЭК» (далее – АС) Региональной энергетической комиссии Омской области (далее – РЭК), меры и средства поддержания непрерывности работы и восстановления работоспособности ИС.

1.2. Целью настоящей Инструкции является обеспечение превентивной защиты элементов ОИ от предотвращения потери защищаемой информации.

1.3. Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей АС организация, имеющих доступ к ресурсам ОИ, а также основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящей Инструкции осуществляется по мере необходимости.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор безопасности ОИ.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

2.1. В настоящей Инструкции под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ОИ,

предоставляемых пользователям ОИ, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей.
- в результате преднамеренных действий пользователей и третьих лиц.
- в результате нарушения правил эксплуатации технических средств ОИ.
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале учета событий информационной безопасности».

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники организация (администратор безопасности, администратор, ответственный за эксплуатацию объекта информатизации), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ И ВОССТАНОВЛЕНИЯ РЕСУРСОВ ПРИ ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ

3.1. Технические меры

1) К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения АИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ОИ включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

2) Все критичные помещения организация (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

3) Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ОИ в

помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

4) Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

5) Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на машинные носители (CD, DVD-диски, жесткие диски, USB Flash-накопитель и т.п.).

6) Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для информации, содержащей сведения, составляющие государственную тайну – не реже раза в месяц;
- для технологической и другой информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ОИ – каждый раз при внесении изменений в эталонные копии (выход новых версий).

7) Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть зарегистрированы и пронумерованы (номером носителя, датой проведения резервного копирования).

Носители должны храниться в запираемом металлическом шкафу.

Носители должны храниться не менее года, для возможности восстановления данных.

Ответственный за организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации объекта информатизации АС: начальник отдела информационного обеспечения РЭК.

Приложение № 3
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
ответственного за эксплуатацию объекта информатизации автоматизированной системы «РЭК» Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет общие функции, права и обязанности
ответственного за эксплуатацию объекта информатизации по вопросам обеспечения защиты информации при разработке документов, содержащих сведения, составляющие государственную тайну, на данном объекте информатизации.

1.2. Настоящая Инструкция разработана на основании действующих нормативных документов по вопросам защиты информации, содержащих сведения, составляющие государственную тайну.

2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

2.1. Контроль за выполнением требований, действующих нормативных и руководящих документов и защиты сведений, составляющих государственную тайну, при проведении работ на объекте информатизации.

2.2. Контроль доступа лиц в помещение, где размещен объект информатизации (ОИ) автоматизированная система (АС) «РЭК» (далее – АС) в соответствии со списком лиц, допущенных в помещение (постоянно или временно).

2.3. Контроль доступа пользователей к работе в ОИ АС (в соответствии со списком допущенных сотрудников).

2.4. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ и устройств ОИ АС.

2.5. Организация технического обслуживания (ремонта, модернизации) ОИ АС и других технических средств, установленных на объекте информатизации.

2.6. Взаимодействие с администратором безопасности ОИ АС по вопросам обеспечения правильного использования пользователями СЗИ от НСД и контроля доступа этих пользователей к работе в ОИ АС.

2.7. Ведение и хранение документации на объекте информатизации. Хранение копий лицензионной версии ОС и СЗИ от НСД, копий настроек СЗИ от НСД.

2.8. Организация и контроль печати на принтере документов,

разработанных в АС.

2.9. Контроль за соблюдением установленных правил и параметров регистрации и учета бумажных и машинных носителей информации и документов.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. Требовать от работников соблюдения установленной технологии обработки информации, содержащей сведения, составляющие государственную тайну и исполнения настоящей Инструкции.

3.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа.

3.3. Требовать от пользователей, администратора безопасности прекращения обработки информации на объекте информатизации в случае:

- нарушения установленного порядка работ,
- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСТЭК России,
- получения информации о возможном проведении технической разведки в отношении объекта информатизации.

4. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

4.1. Обеспечивать правильное функционирование и поддерживать работоспособность технических средств и СЗИ на объекте информатизации в пределах, возложенных на него функций.

4.2. В случае отказа технических средств на объекте информатизации принимать меры по их восстановлению.

4.3. Проводить инструктаж пользователей по правилам работы на объекте информатизации в пределах компетенции этих пользователей.

4.4. Не реже одного раза в месяц проверять наличие пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ АС и ее устройств.

4.5. Немедленно докладывать председателю РЭК или лицу, исполняющему его обязанности, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности на ОИ.

4.6. Вести и хранить документацию на объекте информатизации, копии лицензионной версии ОС и СЗИ от НСД, копии настроек СЗИ от НСД, в соответствии с требованиями нормативных документов.

4.7. Контролировать соблюдение пользователями АС установленных правил и параметров печати, регистрации и учета документов, а также

регистрации и учета бумажных и машинных носителей информации.

4.8. Требовать от пользователей и администратора безопасности прекращения обработки информации в ОИ АС при появлении информации о возможном проведении технической разведки в отношении объекта информатизации.

4.9. Приостанавливать работу с информацией, содержащих сведения, составляющие государственную тайну, на объекте информатизации в случае окончания срока действия сертификата соответствия ФСТЭК России на любое СЗИ из используемых на объекте информатизации до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию объекта информатизации, для принятия совместного решения.

4.10. Ответственный за эксплуатацию автоматизированной системы «РЭК»: начальник отдела информационного обеспечения РЭК.

Приложение № 4
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
по организации парольной защиты объекта информатизации
автоматизированной системы «РЭК»
Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей пользователей (администратора) на объекте информатизации (ОИ) автоматизированной системе «РЭК» (далее – АС) Региональной энергетической комиссии Омской области (далее – РЭК), предназначенных для обработки конфеденцеальной информации.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей пользователей на ОИ возлагается на администратора безопасности (далее - администратора).

2. ПРАВИЛА ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

2.1. Аутентификация авторизированных субъектов доступа осуществляется с помощью парольной защиты (логин + пароль), электронных ключей, комбинированных методов аутентификации (двухфакторная аутентификация) и других программно-технических средств разграничения доступа пользователей. Способ аутентификации авторизированных пользователей определяется в соответствии с категорией обрабатываемой информации.

2.2. При регистрации нового пользователя администратор безопасности должен назначить для него пароль, персональный код либо другую уникальную информацию для доступа к информационным ресурсам объекта информатизации.

2.3. Каждый пароль должен выбираться и генерироваться пользователем и администратором с учетом следующих требований:

- длина пароля должна быть не менее 8 **символов**;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #. $, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- личный пароль пользователь не имеет права сообщать никому.

Администратор несет ответственность за обеспечение процесса генерации пароля, не соответствующего данным требованиям.

2.4. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

2.5. Плановая смена пароля пользователя должна проводиться регулярно, не реже одного раза в 60 дней.

2.6. Внеплановая смена пароля в случае прекращения полномочий сотрудника (увольнение, переход на другую работу и т.п.) должна производиться администратором немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.7. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администратора (увольнение, переход на другую работу и т.п.).

2.8. Каждый пользователь несет ответственность за неразглашение личного пароля третьим лицам и сохранность персонального идентификатора. Хранение пользователем своих паролей и (или) идентификаторов на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе администратора в опечатанном личной печатью пенале (конверте).

2.9. 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 безопасности для получения нового пароля.

2.10. Если пользователь заметит несанкционированное появление, изменение или удаление информации, он должен немедленно сообщить об обнаруженных изменениях руководителю структурного подразделения и администратору безопасности.

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

2.12. При оставлении рабочего места необходимо завершить открытую пользовательскую сессию либо использовать функцию «временной блокировки» рабочей станции (сочетание клавиш Windows + L).

2.13. Пользователям запрещается:

- передача личного пароля посторонним лицам, в том числе сотрудникам РЭК;

- запись личного пароля доступа на материальные носители в открытом виде;

- оставлять без присмотра рабочее место с открытой пользовательской сессией.

2.14. В случае утраты надежности (компрометации) личного пароля, либо подозрения о компрометации пароля, пользователь обязан незамедлительно поставить об этом в известность администратора безопасности для исключения возможности утечки информации и принятия мер по внеплановой смене личного пароля.

2.15. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2.16. Любые действия пользователей и посторонних лиц нарушающие требования настоящей Инструкции, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.

2.17. Каждый сотрудник Региональной энергетической комиссии Омской области несет персональную ответственность за обеспечение информационной безопасности на своем рабочем месте.

2.18. Пользователи и Администраторы несут ответственность, установленную действующим законодательством Российской Федерации за разглашение сведений, составляющих государственную тайну, ставших известными им в процессе выполнения своих должностных обязанностей.

2.19. Ответственный за организацию парольной защиты: начальник отдела информационного обеспечения РЭК.

Приложение № 5
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
по проведению антивирусного контроля объекта информатизации автоматизированной системы «РЭК» Региональной энергетической комиссии Омской области

1. Настоящая инструкция предназначена для администратора безопасности объекта информатизации (ОИ) автоматизированной системы (АС) «РЭК» Региональной энергетической комиссии Омской области, ответственного за эксплуатацию ОИ и пользователей АС.

2. В целях обеспечения сохранности и целостности данных в АС вводится контроль за отсутствием в программной и информационной среде АС компьютерных вирусов (антивирусный контроль).

3. К применению в АС допускается лицензионное антивирусное средство защиты информации: программное изделие «Dr.Web Enterprise Security Suite».

4. На АС запрещается установка любого ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности АС, а в случае его отсутствия - на ответственного за эксплуатацию ОИ в рамках его прав доступа.

6. Администратор безопасности АС обязан осуществлять периодическое (не реже одного раза в месяц) обновление антивирусных средств и баз, а также контроль их работоспособности.

7. Администратор безопасности АС обязан проводить периодическое (не реже одного раза в неделю) тестирование всего установленного ПО и информационных файлов на предмет отсутствия компьютерных вирусов.

8. При обнаружении компьютерного вируса администратор безопасности АС проводит лечение заражённых файлов с использованием штатных антивирусных средств, затем повторяет процедуру проверки (сканирования) программной среды (в том числе информационных файлов) и всех носителей, которые могли быть заражены.

9. В случае обнаружения на отчуждаемом носителе информации нового вируса, не поддающегося уничтожению или излечению, администратор безопасности АС запрещает использование этого носителя до появления антивирусных средств, позволяющих уничтожить новый вирус.

10. Пользователи АС перед началом работы с отчуждаемыми носителями информации (CD-диск, USB – флэш-накопитель) обязаны проверить их на наличие (отсутствие) компьютерных вирусов.

11. Права на запуск антивирусных программ в режиме проверки должны

быть предоставлены всем пользователям АС. Ярлык для запуска антивирусной программы должен быть вынесен на «рабочий стол» Windows или в области часов на рабочей панели.

12. При обнаружении компьютерного вируса пользователь АС обязан немедленно поставить в известность администратора безопасности АС (в случае его отсутствия - ответственного за эксплуатацию объекта информатизации) и прекратить работу на АС.

Приложение № 6
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в объект информатизации автоматизированную систему «РЭК» Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в объект информатизации (ОИ) автоматизированную систему «РЭК» Региональной энергетической комиссии Омской области (далее - АС, РЭК), защищённой от несанкционированного доступа и предназначенной для обработки и хранения информации, содержащей сведения, составляющие государственную тайну.

Данные работы проводятся только с разрешения председателя РЭК или лица, исполняющего его обязанности, после согласования с ответственным за эксплуатацию объекта информатизации и администратором безопасности АС.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ ПО ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ, РЕМОНТУ, МОДЕРНИЗАЦИИ

2.1. В случаях, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) АС или иных технических средств, использующихся для обработки и хранения информации, содержащей сведения, составляющие государственную тайну, ответственный за эксплуатацию ОИ представляет служебную записку на имя руководителя организации, в которой:

- Указывает название и номер АС (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;
- Обосновывает необходимость технического обслуживания (модернизации);
- Указывает планируемые место и сроки работ, режим их проведения;
- Перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью предотвращения несанкционированного доступа к конфиденциальной информации.

2.2. Запрещается выносить АС с территории РЭК без согласования с ответственным за эксплуатацию ОИ и разрешения председателя РЭК.

2.3. Вскрытие печатей на корпусе АС или технических средств (систем) и последующее опечатывание производится комиссионно в присутствии ответственного за эксплуатацию ОИ и администратора безопасности АС.

2.4. В акте указывается:

- Номер (название) помещения, в котором проводились работы
- Дата и время начала и окончания работ
- Лица, присутствовавшие при вскрытии корпуса АС и обслуживании (ремонте, модернизации)
- Наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия корпуса АС (технического средства, систем)
- Установленные неисправности
- Виды и результаты проведенных работ
- Заменённые или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков
- Какими печатями (пломбами) и в каких местах АС (устройство) опечатано по окончании работ
- Необходимость проведения дополнительных специальных исследований (сертификации) АС (технического средства, системы)
- Иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.5. Если для ремонта (модернизации) АС (технического средства, системы, узла ПЭВМ) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.6. Перед отправкой АС (технического средства, системы, узла ПЭВМ) администратор безопасности АС обязан снять с АС жёсткий диск (определить его на хранение в РСП) и гарантированно удалить информацию с иных устройств памяти АС (технического средства, системы).

2.7. По факту снятия жёсткого диска и передачи его на хранение составляется акт.

2.8. По факту удаления информации составляется акт.

2.9. В случае, если не имеется возможности гарантированно удалить информацию с иных устройств памяти АС (технического средства, системы) сертифицированными средствами, эти устройства опечатываются и хранятся в РСП с соблюдением требований безопасности информации.

2.10. Ремонт и замена жёсткого диска производится с соблюдением требований п.п. 2.5-2.7 настоящей инструкции в присутствии администратора АС.

При диагностике и ремонте жёсткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

Приложение № 7
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
пользователя объекта информатизации
автоматизированной системы «РЭК» Региональной энергетической комиссии Омской области по обеспечению безопасности обработки информации при возникновении внештатных ситуаций

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием объекта информатизации (ОИ) автоматизированной системы (АС) «РЭК» Региональной энергетической комиссии Омской области, меры и средства поддержания непрерывности работы и восстановления работоспособности АС после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов АС от прерывания работы в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- Определение мер защиты от прерывания
- Определение действий восстановления работоспособности АС

1.3. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АС, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- Системы жизнеобеспечения
- Системы обеспечения отказоустойчивости
- Системы резервного копирования и хранения данных
- Системы контроля физического доступа

1.4. Пересмотр настоящего документа осуществляется по мере необходимости.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА АВАРИЙНУЮ СИТУАЦИЮ

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов АС, предоставляемых пользователям АС. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведённых далее.

2.2. Источники угроз:

Технологические угрозы

• Пожар в здании.

• Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения).

• Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением).

• Химический выброс в атмосферу.

Внешние угрозы.

• Сбои общественного транспорта.

• Эпидемия.

• Массовое отравление персонала.

Стихийные бедствия.

• Удар молнии.

• Сильный снегопад.

• Сильные морозы.

• Просадка грунта (подмыв грунтовых вод) с частичным обрушением здания.

• Затопление водой в период паводка.

• Наводнение, вызванное проливным дождем.

• Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

Телекоммуникационные и IT угрозы.

• Сбой IT – систем.

Угрозы, связанные с человеческим фактором.

• Ошибка персонала, имеющего доступ к АС.

• Нарушение конфиденциальности, целостности и доступности конфиденциальной информации.

Угрозы, связанные с внешними поставщиками.

• Отключение электроэнергии.

• Физический разрыв линий.

2.3. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учёту мероприятий по контролю за ситуацией».

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, сотрудники организация (ответственный за эксплуатацию ОИ и администратор безопасности АС) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.5. Уровни реагирования на инцидент.

При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – *Незначительный инцидент.* Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов АС и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 – *Авария.* Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов АС и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

• Отказ элементов АС и средств защиты из-за повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей.

• Отказ элементов АС и средств защиты из-за отсутствия ответственного за эксплуатацию ОИ и администратора безопасности АС более чем на сутки из-за: химического выброса в атмосферу, сбоев общественного транспорта, эпидемии, массового отравления персонала, сильного снегопада, сильных морозов.

Уровень 3 – *Катастрофа.* Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов АС и средств защиты, а также к угрозе жизни пользователей АС, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности АС и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты

• Пожар в здании.

• Взрыв.

• Просадка грунта с частичным обрушением здания.

3. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ И ВОССТАНОВЛЕНИЯ РЕСУРСОВ ПРИ ВОЗНИКНОВЕНИИ АВАРИЙНЫХ СИТУАЦИЙ

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

• Системы жизнеобеспечения.

• Системы обеспечения отказоустойчивости.

• Системы резервного копирования и хранения данных.

• Системы контроля физического доступа.

Системы жизнеобеспечения АС включают:

• Пожарные сигнализации и системы пожаротушения.

• Системы вентиляции и кондиционирования.

• Системы резервного питания.

Все критичные помещения организации (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации. Порядок предотвращения потерь информации и организации системы жизнеобеспечения АС описан в Порядке резервирования и восстановления работоспособности технический систем и программного обеспечения, баз данных и средств защиты информации.

3.2. Организационные меры

Ответственные лица за реагирование знакомят всех сотрудников организации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трёх рабочих дней с момента выхода нового сотрудника на работу. По окончанию ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность. Должно быть проведено обучение должностных лиц организации, имеющих доступ к ресурсам АС, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

• Оказание первой медицинской помощи.

• Пожаротушение.

• Эвакуация людей.

• Защита материальных и информационных ресурсов.

• Методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию.

• Выключение оборудования, электричества, водоснабжения, газоснабжения.

Ответственный за эксплуатацию ОИ и администратор безопасности АС должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов АС. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Приложение № 8
к приказу Региональной энергетической
комиссии Омской области
от 7 марта 2023 года № 3-П

ИНСТРУКЦИЯ
пользователя объекта информатизации
автоматизированная система «РЭК»
Региональной энергетической комиссии Омской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет общие положения работы пользователей на защищенном от несанкционированного доступа объекта информатизации (ОИ) автоматизированной системе «РЭК» Региональной энергетической комиссии Омской области (далее – АС, РЭК) при обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

1.2. Пользователем является каждый сотрудник организация, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, подлежащей защите и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации (далее – СЗИ).

1.3. Допуск пользователей для работы в АС осуществляется ответственным за эксплуатацию объекта информатизации в соответствии со списком пользователей, допущенных к обработке соответствующей информации.

1.4. Присвоение пользователю полномочий доступа к ресурсам компьютера и определение возможного времени работы пользователя в АС осуществляется администратором безопасности АС при первичной регистрации пользователя в АС.

1.5. Вход пользователя в систему осуществляется на основе ввода (по запросу системы) имени, присвоенного при первичной регистрации администратором безопасности АС, и ввода личного пароля длиной не менее восьми символов, определяемого конкретным пользователем.

1.6. Пользователь в своей работе руководствуется настоящей инструкцией, Руководством по защите информации в РЭК, руководящими и нормативными документами ФСТЭК России, ФСБ России, Правительства Российской Федерации, Министерства связи и массовых коммуникаций Российской Федерации и регламентирующими документами РЭК.

2. ОСНОВНЫЕ ФУНКЦИИ ПОЛЬЗОВАТЕЛЯ АС

2.1. В процессе первичной регистрации для работы в АС пользователь заявляет администратору безопасности АС перечень необходимых для его работы ресурсов и состав необходимого общесистемного программного обеспечения для решения поставленных задач.

2.2. Резервное копирование, уничтожение и восстановление информации осуществляется пользователем в рамках выделенных полномочий, либо администратором безопасности АС.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ АС

3.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС, присвоенными администратором безопасности АС данному пользователю. При этом для обработки и хранения файлов, содержащих информацию ограниченного доступа, разрешается использовать только специально выделенные каталоги в соответствующих разделах АС.

3.2. Хранение копий файлов, содержащих информацию ограниченного доступа, разрешается на учтенных в журнале учета машинных носителях информации (МНИ) с учетом безопасности сохранности информации.

3.3. По всем возникающим вопросам при работе в АС обращаться к администратору безопасности АС.

4. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ АС

4.1. Ознакомиться с Руководством по защите информации в РЭК, принятых процедур работы с элементами информационных систем, АС и СЗИ.

4.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, Руководства по защите информации в РЭК, приказов и распоряжений, регламентирующих порядок действий по защите информации.

4.3. Следовать установленным процедурам поддержания режима безопасности информации.

4.4. Знать и соблюдать установленные требования по режиму обработки информации ограниченного доступа, учету, хранению и пересылке носителей информации, обеспечению безопасности информации, а также руководящих и организационно-распорядительных документов.

4.5. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (не реже раза в 60 дней) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно. В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к администратору безопасности.

4.6. В свое отсутствие пользователи АС обязаны выключать АС или блокировать ее. После этого разблокировка АС производится только после ввода своего пароля пользователем.

4.7. Сотрудники организация, использующие технические средства аутентификации, обязаны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а также исключить возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

4.8. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к администратору безопасности АС.

5. В ПРОЦЕССЕ РАБОТЫ ПОЛЬЗОВАТЕЛЮ ЗАПРЕЩАЕТСЯ

5.1. Разглашать защищаемую информацию третьим лицам.

5.2. Самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

5.3. Подключать к рабочей станции и корпоративной информационной сети личные, либо неучтенные мобильные устройства и носители информации, а также записывать (копировать) на них защищаемую информацию.

5.4. Сообщать посторонним лицам личные ключи и атрибуты доступа к ресурсам АС.

5.5. Привлекать посторонних лиц для производства ремонта или настройки АС, без согласования с администратором безопасности АС.

5.6. Проводить обработку защищаемой информации при неисправно работающих, либо выключенных средствах защиты информации.

5.7. Допускать к работам в АС лиц, не имеющих допуска к этим работам.

5.8. Осуществлять попытки несанкционированного доступа к ресурсам системы и других пользователей.

5.9. Пытаться подменять функции администратора безопасности АС по перераспределению времени работы и полномочий доступа к ресурсам АС.

6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ АС

6.1. Каждый сотрудник организация несет персональную ответственность за обеспечение информационной безопасности на своем рабочем месте.

6.2. Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации,

если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ.

6.3. Пользователи информационной системы несут ответственность, установленную действующим законодательством Российской Федерации за разглашение информации ограниченного распространения, не содержащей сведений, составляющих государственную тайну, ставших известными им в процессе выполнения своих должностных обязанностей.