УТВЕРЖДЕНА

приказом директора
ОГБУ «КЦСО ЕАО»
от «02» 07 2024 г. № 184

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
по обеспечению безопасности при возникновении нештатных ситуаций в ИСПДн областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

I. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».

1.2. Данная инструкция определяет наиболее распространенные нештатные ситуации, порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее – ИСПДн), а также меры, принимаемые для восстановления работоспособности ИСПДн после возникновений нештатных ситуаций, связанных с работой в ИСПДн областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области» (далее – ОГБУ «КЦСО ЕАО», Учреждение).

1.3. Пользователем ИСПДн (далее – Пользователь) является работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн согласно приказу об утверждении списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИСПДн, для выполнения своих

должностных обязанностей.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до работников под личную подпись. Пользователь должен быть предупрежден о возможной ответственности за нарушение.

1.6. Действие настоящей Инструкции распространяется также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении нештатных ситуаций, в том числе:

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

1.7. Нештатная ситуация становится возможной в результате реализации одной либо нескольких угроз, приведенных в Приложении № 1.

II. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента.

Критичность оценивается на основе следующей классификации:

1. Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на работоспособность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

2. Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками. К авариям относятся следующие инциденты: отказ элементов ИСПДн и средств защиты из-за повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей; неполадки, связанные с перепадами напряжения в сети электропитания.

3. Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы, которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более. К катастрофам относятся следующие инциденты: пожар в здании; взрыв; просадка грунта с частичным обрушением здания.

III. Общий порядок действий при возникновении нештатных ситуаций

3.1. В настоящей Инструкции под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также с вероятностью потери защищаемой информации.

3.2. К нештатным относятся следующие ситуации:

- сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т.п.);
- отключение электричества;
- сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т.п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т.п.);
- обнаружение вируса;
- обнаружение утечки информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т.п.);
- взлом системы (web-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т.п.);
- компрометация ключей (утеря носителя ключевой информации и т.п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место; взлом учетной записи пользователя);
- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т.п.)
- физическое повреждение локально-вычислительной сети (далее – ЛВС) или персонального компьютера (далее – ПК) (не включается ПК, при попытке включения отображается синий или черный экран, повреждены провода и т.п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИСПДн и возможность потери защищаемой информации, и названные таковыми пользователем ИСПДн или ответственным за ИСПДн.

3.3. При возникновении нештатных ситуаций во время работы,

обнаруживший нештатную ситуацию, немедленно ставит в известность лицо, ответственное за техническую защиту информации в Учреждении (далее – специалиста по технической поддержке). В случае, если поставить в известность вышеуказанное лицо не представляется возможным, составляется служебная записка в произвольной форме с описанием нештатной ситуации, и администратору информационной безопасности.

3.4. Специалист по технической поддержке проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность директора ОГБУ «КЦСО ЕАО» для определения дальнейших действий.

3.5. В кратчайшие сроки, не превышающие одного рабочего дня, директор учреждения и ответственные специалисты предпринимают меры по восстановлению работоспособности ИСПДн. Предпринимаемые меры согласуются с вышестоящим руководством.

Директор учреждения в первую очередь выясняет причины нештатной ситуации и предпринимает действия по её устранению, при необходимости привлекает ответственных специалистов.

По мере необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3.6. По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учёта нештатных ситуаций ИСПДн».

3.7. При необходимости проводится служебное расследование по факту возникновения нештатной ситуации и выяснению её причин.

IV. Особенности действий при возникновении наиболее распространённых нештатных ситуаций

4.1. Сбой в системе жизнеобеспечение здания (электро-, тепло-, водоснабжение, водоотведение): директор учреждения подключает к работе специалистов (электрика, сантехника, рабочего), которые проверяют работоспособность соответствующего оборудования и устраняют поломку.

Специалист по технической поддержке и работник, у которого произошла нештатная ситуация, проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения (далее – ПО), а также проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

4.2. Сбой программного обеспечения, обнаружение потери, уничтожения, модифицирования, блокирования, копирования, потери данных, иных причин: ответственные специалисты выясняют причину и последствия сбоя. Проводят мероприятия по устранению последствий сбоя: антивирусную проверку,

целостность и работоспособность ПО, целостность и работоспособность оборудования и другие.

При необходимости производится восстановление ПО и данных из последней резервной копии. Если исправить ошибку своими силами не удалось, то ответственные специалисты обращаются за помощью к специалисту по технической поддержке.

4.3. Сбой в ЛВС, выход из строя сервера: ответственные специалисты поручают сотрудникам, по функциональным обязанностям отвечающим за работу соответствующего оборудования, определить и устранить возникшие в оборудовании проблемы.

Специалист по технической поддержке проводит меры по немедленному вводу в действие резервного сервера (при наличии) для обеспечения непрерывной работы пользователей ИСПДн. В случае необходимости производится восстановление ПО и данных из последней резервной копии.

4.4. Потеря данных: при обнаружении потери данных, специалист по технической поддержке проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости производится восстановление ПО и данных резервной копии.

4.5. Обнаружен вирус: производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «заражённый» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится ответственным за ИСПДн. Результатом анализа может быть попытка сохранения (спасения) данных, т.к. после перезагрузки АРМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохранённые данные также необходимо подвергнуть проверке на наличие вируса.

При обнаружении вируса следует руководствоваться Инструкцией антивирусной защиты. После ликвидации необходимо провести внеочередную антивирусную проверку на всех АРМ с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных данных из резервных копий. Проводится служебное расследование по факту появления вируса.

4.6. Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации необходимо сообщить администратору информационной безопасности, а также ответственному за организацию обработки персональных данных в Учреждении. Провести служебное расследование. Если утечка информации произошла по техническим причинам,

проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновению.

4.7. Взлом системы или несанкционированный доступ (далее – НСД). При обнаружении взлома сервера проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянские закладки. Учитывая, что программные закладки могут быть не обнаружены антивирусом ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий.

4.8. Попытка несанкционированного доступа. При обнаружении утечки информации необходимо поставить в известность администратора информационной безопасности, а также ответственного за организацию обработки персональных данных в Учреждении. Рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такое обновления.

В случае обнаружения злоумышленника, неправомерно копирующего, либо изменяющего защищаемую информацию, ответственные специалисты прерывают несанкционированный процесс, блокируют доступ к ИСПДн. Создается комиссия для расследования инцидента.

4.9. Компрометация ключей. При обнаружении утечки информации необходимо сообщить администратору информационной безопасности. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

4.10. Компрометация пароля. При обнаружении утечки информации необходимо сообщить администратора информационной безопасности, сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять меры по минимизации возможного (или нанесенного) ущерба.

4.11. Физическое повреждение ЛВС или ПК. Необходимо сообщить администратора информационной безопасности. Определить причины повреждения ЛВС или ПК и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод из строя оборудования, провести служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. При необходимости провести меры по восстановлению ПО и данных из резервных копий.

В случае ошибки пользователей при эксплуатации технических средств, программных средств и систем защиты информации, повлекших нарушение работоспособности, проводится анализ и идентификация причин инцидента, определяется ущерб, нанесенный нештатной ситуацией, восстанавливается работоспособность системы.

4.12. Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими действия при ЧС: все пользователи выключают свои персональные компьютеры. Ответственные специалисты принимают решения о выключении серверов, сетевого оборудования и принимают меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества.

V. Меры против возникновения нештатных ситуаций

5.1. Специалистом по технической поддержке не реже 1 раза в год должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

5.2. В общем случае, для предотвращения нештатных ситуаций необходимо чёткое соблюдение требований нормативных документов и инструкций по эксплуатации оборудования и ПО.

5.3. Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

- сбой программного обеспечения – применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на АРМ;

- отключение электричества – использовать источники бесперебойного питания на критически важных участках;

- сбой ЛВС – обеспечение бесперебойной работы ЛВС путём применения надежных сетевых технологий и резервных систем;

- выход из строя сервера – применять надежные программно-технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов;

- потеря данных – периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации, обеспечить резервное копирование данных;

- обнаружение вируса – соблюдать требования Инструкции по антивирусной защите;

- утечка информации – применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию

системы защиты информации;

- попытка несанкционированного доступа – по возможности установить регистрацию попыток НСД на всех участках, где возможен несанкционированный доступ, с оповещением администратора информационной безопасности о попытках НСД;

- компрометация паролей – соблюдать требования «Инструкции пользователя информационной системы персональных данных»;

- физическое повреждение ЛВС или ПК – физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним;

- стихийное бедствие – проводить обучающие собрания и тренировки работников по вопросам гражданской обороны.

VI. Заключительные положения

6.1. Настоящая Инструкция вступает в силу в силу с момента утверждения руководителем Учреждения.

6.2. Срок действия настоящей Инструкции не ограничен.

6.3. По мере необходимости в настоящую Инструкцию могут быть внесены дополнения и изменения в соответствии с законодательством РФ.

Приложение № 1

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
Стихийные бедствия	
1	Удар молнии
2	Сильные морозы, снегопад, паводок, наводнение
3	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
Угрозы, связанные с внешними поставщиками	
1	Отключение электроэнергии
2	Физический разрыв внешних каналов связи
3	Сбой в работе Интернет-провайдера
Угроза, связанная с человеческим фактором	
1	Ошибка персонала, имеющего доступ к серверной
2	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Иные угрозы	
1	Сбой технических средств ИСПДн
2	Сбой информационных систем или программного обеспечения
3	Массовые беспорядки
4	Эпидемия