

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 199
ПРИМОРСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**

УТВЕРЖДАЮ

Врио Директора
ГБОУ школа № 199




Протасова О. В.
18 июля 2023 г.

**ИНСТРУКЦИЯ
пользователю в случае возникновения нештатных ситуаций
в ГБОУ школа №199 Приморского района**

1. Общие положения

1.1. Настоящая Инструкция определяет действия сотрудников по применению основных мер, методов и средств сохранения (поддержания) работоспособности АИСУ «Параграф» (АИСУ) при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности АИСУ и ее основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1.2. Под **кризисной ситуацией** понимается ситуация, возникшая в результате нежелательного воздействия на АИСУ, не предотвращенная средствами защиты. Кризисная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, пожаров, аварий, стихийных бедствий и т.п.).

Под **умышленным нападением** понимается кризисная ситуация, которая возникла в результате выполнения злоумышленниками в определенные моменты времени заранее обдуманных и спланированных действий.

Под **случайной (непреднамеренной) кризисной ситуацией** понимается такая кризисная ситуация, которая не была результатом заранее обдуманных действий и возникновение которой, явился результат объективных причин случайного характера, халатности, небрежности или случайного стечения обстоятельств.

По степени серьезности и размерам наносимого ущерба, кризисные ситуации разделяются на следующие категории:

Угрожающая - приводящая к полному выходу АИСУ из строя и ее неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

Серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы) к критическим не относятся. Действия в случае возникновения таких ситуаций предусмотрены Планом защиты.

1.3. Кризисные ситуации, предусмотренные планом обеспечения непрерывной работы и восстановления

1. К *угрожающим кризисным ситуациям* относятся:

- нарушение подачи электроэнергии в здании;
- выход из строя файлового сервера (с потерей информации);
- выход из строя файлового сервера (без потери информации);
- частичная потеря информации на сервере без потери его работоспособности;
- выход из строя локальной сети;

2. К *серьезным кризисным ситуациям* относятся:

- выход из строя рабочей станции (с потерей информации);

- выход из строя рабочей станции (без потери информации);
- частичная потеря информации на рабочей станции без потери ее работоспособности;

3. К *ситуациям, требующим внимания*, относятся:

- несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

1.4. Источники информации о возникновении кризисной ситуации:

- пользователи, обнаружившие несоответствия или иные подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;
- средства защиты, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Меры обеспечения непрерывной работы и восстановления автоматизированной системы

Непрерывность процесса функционирования АИСУ и своевременность восстановления ее работоспособности достигается:

- проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывности работы АИСУ;
- строгой регламентацией процесса обработки информации и действий персонала системы, в том числе в кризисных ситуациях;
- назначением и подготовкой должностных лиц, отвечающих за организацию и осуществление практических мероприятий по обеспечению непрерывности работы АИСУ;
- применением различных способов резервирования информационных ресурсов системы;
- эффективным контролем за соблюдением требований по обеспечению непрерывности работы АИСУ должностными лицами и ответственным;
- постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты;

3. Общие требования

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться. Дальнейшие действия по устранению причин нарушения работоспособности АИСУ, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая кризисная ситуация должна анализироваться администратором безопасности, и по результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п.

Серьезная и угрожающая кризисная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе, должны иметь эталонные (дистрибутивные) копии.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает, возможно, более полное восстановление программных, аппаратных, информационных и других поврежденных компонентов системы.

В случае возникновения любой кризисной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

4. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению системы

Действия персонала в кризисной ситуации зависят от степени ее тяжести.

4.1. В случае возникновения ситуации, требующей внимания, сотрудник должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность руководство и сотрудников ИТ отдела Школы.

4.2. В случае возникновения угрожающей или серьезной критической ситуации действия персонала включают следующие этапы:

- немедленная реакция;
- частичное восстановление работоспособности и возобновление обработки;
- полное восстановление системы и возобновление обработки в полном объеме;
- расследование причин кризисной ситуации и установление виновных.

4.3. Этапы включают следующие действия:

4.3.1. В качестве немедленной реакции:

- обнаруживший факт возникновения кризисной ситуации оператор АРМ обязан немедленно оповестить об этом сотрудника ИТ отдела Школы;
- сотрудник ИТ отдела должен поставить в известность операторов АРМ о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной

ситуации и ориентировочном времени возобновления обработки.

4.3.2. При частичном восстановлении работоспособности (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) и возобновлении обработки:

- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих (под)систем.
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить поврежденное критичное программное обеспечение, используя эталонные (страховые) копии;
- восстановить необходимые данные, используя страховые копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить операторов смежных (под)систем о готовности к работе.
-

Затем необходимо внести все изменения данных за время с момента создания последней страховой копии (за текущий период, операционный день), для чего должен осуществляться "откат" на основании информации из журналов транзакций либо все связанные с поврежденной (под)системой пользователи должны повторить действия выполненные в течение последнего периода (дня).

4.3.3. Для полного восстановления в период неактивности системы:

- восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;
- восстановить все поврежденные данные, используя страховые копии и журналы транзакций;
- настроить средства защиты подсистемы в соответствии с планом защиты;

4.3.4. Далее необходимо провести расследование причин возникновения кризисной ситуации. Расследование кризисной ситуации производится группой, назначаемой руководством учреждения. Выводы группы докладываются непосредственно руководству учреждения.