УТВЕРЖДАЮ

Ректор ПГНИУ

_____/Макарихин И.Ю.

«___» _____ 20__ г.

ИНСТРУКЦИЯ

администратора информационной безопасности ИСПД на случай возникновения внештатных ситуаций

1. Общие положения

1.1. Настоящая Инструкция определяет действия администратора информационной безопасности ИСПД по применению основных мер, методов и средств сохранения (поддержания) работоспособности ИСПД, используемой в ПГНИУ, при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПД и их основных компонентов.

1.2. Под кризисной ситуацией понимается ситуация, возникшая в результате нежелательного воздействия на ИСПД, 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 причиной возникновения 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 ИСПД из строя и их 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.

Требующая внимания - 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).

1.3. 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 или сигнализации, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. 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 ИСПД, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями работников.

Каждая кризисная ситуация должна анализироваться администратором информационной 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.д.

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 ИСПД 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.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает восстановление программных, аппаратных, информационных и других поврежденных компонентов системы. Для восстановления используются архивные и резервированные данные.

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

Расследование кризисной ситуации производится группой, назначаемой ректором ПГНИУ. Выводы группы докладываются непосредственно ректору ПГНИУ.

Если причиной угрожающей или серьезной кризисной ситуации явились недостаточно жесткие меры защиты и контроля, а ущерб превысил установленный уровень, то такая ситуация является основанием для полного пересмотра планов обеспечения непрерывной работы и восстановления.

4. Обязанности и действия администратора информационной безопасности по обеспечению непрерывной работы и восстановлению ИСПД

Действия администратора информационной безопасности в кризисной ситуации зависят от степени ее тяжести.

4.1. В случае возникновения ситуации, требующей внимания, администратор информационной безопасности должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность руководителя подразделения.

4.2. В случае возникновения угрожающей или серьезной критической ситуации действия администратора информационной безопасности включают следующие этапы:

4.2.1. Немедленная реакция - администратор информационной безопасности должен**:**

- поставить в известность пользователей, обрабатывающих информацию о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- оповестить о сложившейся ситуации системного программиста или администратора, обслуживающего ИСПД и руководителя подразделения;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.

4.2.2. Частичное восстановление 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 подсистем.

- 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 резервные копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить администраторов смежных подсистем о готовности к работе.

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

4.2.3. Полное восстановление 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;

4.2.4. Далее необходимо провести расследование причин возникновения кризисной ситуации.