Приложение № 4
к Приказу № 2132-О
от 08 декабря 2016 г.

Министерство образования и науки
Российской Федерации

Инструкция пользователей информационных систем персональных данных на случай возникновения внештатных ситуаций

в федеральном государственном бюджетном
образовательном учреждении
высшего образования
«Уфимский государственный
авиационный технический университет»

1. Общие положения

1.1. Настоящая Инструкция определяет действия работников по применению основных мер, методов и средств сохранения (поддержания) работоспособности информационной системы персональных данных (далее - ИСПД), используемой в Федеральном государственном бюджетном учреждении высшего образования « Уфимский государственный авиационный технический университет» (далее – Университет), 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. 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 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. Меры обеспечения непрерывной работы и восстановления автоматизированных систем Университета

2.1. Непрерывность процесса функционирования ИСПД и своевременность восстановления их работоспособности достигается:

• проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывности вычислительного процесса;

• строгой регламентацией процесса обработки информации с применением автоматизированных рабочих мест (АРМ) 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 вычислительного процесса;

• четким знанием и строгим соблюдением всеми должностными лицами, использующими средства вычислительной техники, требований руководящих документов по обеспечению непрерывности вычислительного процесса;

• применением различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов ИСПД;

• эффективным контролем за соблюдением требований по обеспечению непрерывности вычислительного процесса должностными лицами и ответственным;

• постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты;

• проведением постоянного анализа эффективности принятых мер и применяемых способов и средств обеспечения непрерывности вычислительного процесса, разработкой и реализацией предложений по их совершенствованию.

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 ИСПД, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая кризисная ситуация должна анализироваться ответственным за безопасность ИСПД, 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 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.

Их местонахождение и сведения об ответственных за их создание, хранение и использование должны быть указаны в документации к ИСПД для служебного пользования. Там же должны быть указаны перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственные за создание, хранение и использование страховых копий данных.

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

Каждая логическая структура, содержащая резервную копию, должна иметь метку, содержащую данные об исходной ИСПД, состав копии, дату снятия копии.

Дублирующие аппаратные ресурсы предназначены для обеспечения работоспособности системы в случае выхода из строя всех или отдельных аппаратных компонентов в результате угрожающей кризисной ситуации. Количество и характеристики дублирующих ресурсов должны обеспечивать выполнение основных задач системой в любой из предусмотренных кризисных ситуаций.

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 Университета. Возглавляет группу ответственный за безопасность ИСПД. Выводы группы докладываются непосредственно ректору Университета.

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, ответственный за безопасность ИСПД должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность ректора Университета.

4.2. В случае возникновения угрожающей или серьезной критической ситуации действия сотрудников 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 пользователь обязан немедленно оповестить об этом ответственного за безопасность ИСПД, по телефону, лично, или по электронной почте;

• ответственный за безопасность ИСПД должен поставить в известность пользователей, обрабатывающих информацию 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. Ответственными за этот этап являются пользователи ИСПД и ответственный за безопасность ИСПД.

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 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 операторов смежных подсистем о готовности к работе.

• 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).

Ответственными за этот этап является ответственный за безопасность ИСПД.

4.3.3.Для полного восстановления в период неактивности системы следует:

• 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;

• о результатах восстановления уведомить администратора системы (базы данных).

Ответственным за этот этап является ответственный за безопасность ИСПД.

4.3.4. Далее необходимо провести расследование причин возникновения кризисной ситуации.

Ответственным за расследование является ответственный за защиту персональных данных в университете.

Отчет о результатах расследования и предложениях по совершенствованию системы необходимо направить ректору Университета.