Приложение 17
к Положению об
информационной безопасности

Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях

1. Общие положения и основные понятия

1. Настоящая Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях в НАО «Евразийский национальный университет» (далее Университет), определяет основные меры, методы и средства сохранения (поддержания) работоспособности информационных систем (далее - ИС) при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИС и ее основных компонентов. Кроме того, он описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

2. Ситуация, возникающая в результате нежелательного воздействия на ИС, приведшая к угрозе информационной безопасности, называется кризисной. Кризисная ситуация может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

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

4. угрожающая - приводящая к полному выходу из строя ИС и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации.

5. К угрожающим кризисным ситуациям относятся:

1) нарушение подачи электроэнергии в здании;

2) выход из строя файлового сервера (с потерей информации);

3) выход из строя файлового сервера (без потери информации);

4) частичная потеря информации на сервере без потери его работоспособности;

5) выход из строя локальной сети (физической среды передачи данных);

6) 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.

6. К серьезным кризисным ситуациям относятся:

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

2) выход из строя рабочей станции (без потери информации);

3) частичная потеря информации на рабочей станции без потери ее работоспособности;
4) стихийные бедствия (пожар, наводнение, ураган и т.д.).

7. Подробное описание о порядке действий пользователей во внештатных (кризисных) ситуациях находится в Приложении 1 к данной инструкции.

8. Источники информации о возникновении кризисной ситуации:

1) пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;

2) средства защиты, обнаружившие кризисную ситуацию;

3) системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Общие требования

9. Все пользователи, работа которых нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, немедленно оповещаются посредством электронной почты администраторами ИС. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

10. Каждая кризисная ситуация анализируется Отделом информационной безопасности (далее ОИБ). По результатам этого анализа вырабатываются предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости проводится расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

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

12. 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. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

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

14. Все программные средства, используемые в системе, имеют эталонные (дистрибутивные) копии.

15. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных отражаются в функциональных обязанностях соответствующих категорий персонала, как правило - это системные администраторы, администраторы автоматизированных рабочих мест, сотрудники Департамента цифрового развития и дистанционного обучения (далее ДЦРиДО), Департамента технического обслуживания (далее ДТО), ОИБ, а также фиксируются в реестре согласно Приложению 2 к данной Инструкции.

3. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению информационных систем

16. Действия персонала в кризисной ситуации зависят от степени ее тяжести.

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

1) немедленная реакция ответственного персонала;

a) В кризисных (внештатных) ситуациях пользователи немедленно оповещаются посредством внутренней электронной почты, устно по телефону или с помощью электронных средств связи сотрудниками, ДЦРиДО, ДТО, ОИБ.

b) В дневное время суток пользователь, обнаруживший внештатную (кризисную) ситуацию, ставит в известность сотрудников ОИБ, или Helpdesk в части технической поддержки информационных ресурсов и систем и серверного обслуживания.

c) В ночное время суток при возникновении внештатной ситуации обнаруживший пользователь должен поставить в известность дежурного сотрудника ДЦРиДО, ДТО и ОИБ, в срочном порядке средствами телефонной связи оповещаются: ответственные руководители структурных подразделений за данный участок работ и ОИБ. Событие в обязательном порядке регистрируется в журнале, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных руководителей структурных подразделений, описание действий, направленных на устранение кризисной ситуации.

2) частичное восстановление работоспособности и возобновление обработки;

3) полное восстановление системы и возобновление обработки в полном объеме;

4) расследование причин возникновения кризисной ситуации и установление виновных;

5) выработка решений по устранению причин и недопущения в последующем подобных фактов нарушений.

18. Контроль за организацией работ в кризисных ситуациях осуществляет ОИБ.

4. Мероприятия по ведению регистрации и описанию внештатных ситуаций

19. Сотрудники ДЦРиДО, ДТО, совместно с ОИБ заводят журнал учета и регистрации внештатных ситуаций. В данном журнале обязательно регистрируются: причины ситуации, ее продолжительность и значение параметров во время нештатной. При необходимости составляется акт и разрабатывается план необходимых корректирующих мер по исправлению критической ситуации.