?????????? ? ??????? ???????? ????????????? ?? ?????????? (??????????) ????????? ? ?????????? «SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Общие положения и основные понятия

2. Общие требования

3. Средства обеспечения непрерывной работы и восстановления

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

Приложение 1

Приложение 2

Приложение 3

1. ????? ????????? ? ???????? ???????

1. Настоящая Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях в Учреждении «SDU University» (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.

Системный администратор информационной системы (далее - СА) – сотрудники Отдела информационно-технической поддержки (далее – ОИТП), которые выполняют функции администрирования серверов и прикладного активного оборудования локальной вычислительной сети, отвечающие за администрирование:

Серверов баз данных (далее - БД);

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.

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

1) 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.

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 (физической среды передачи данных);

2) 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.

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;
- стихийные бедствия (пожар, наводнение, ураган и т.д.).

Более подробное описание о порядке действий пользователей во внештатных (кризисных) ситуациях находится в приложении № 3 данной инструкции.

3. 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. ????? ??????????

1. Все пользователи (сотрудники Университета, студенты Университета, а также сотрудники организаций, выполняющие работы в Университете, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться посредством электронной почты, смс-оповещениями, через громкоговорящую связь. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователями систем.

2. Каждая кризисная ситуация должна анализироваться специалистами ИБ. 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., при необходимости должно проводиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

3. Серьезная и угрожающая кризисная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования в соответствии с утвержденными по Университету правилами, а также восстановления поврежденных программ и наборов данных из резервных копий.

4. 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.

5. 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.

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

7. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала, как правило – это системные администраторы автоматизированных рабочих мест, специалисты информационной безопасности (далее - СИБ).

3. ???????? ??????????? ??????????? ?????? ? ?????????????

1. Структурными подразделениями Университета определяется перечень ИС, подлежащих резервному копированию и резервированию.

2. Резервному копированию подлежит следующая информация:

1) системные программы и сопутствующие наборы данных – не возобновляемые (однократные, эталонные) резервным копированием;

2) прикладное программное обеспечение и сопутствующие наборы данных – не возобновляемые резервным копированием;

3) наборы данных, генерируемые в течение операционного дня и содержащие ценную информацию (системный журнал и т.д.) - периодически возобновляемые резервным копированием, призванному обеспечить долгосрочное сохранение наработанной информации.

3. Безопасность резервных копий обеспечивается:

1) хранением резервных копий вне системы (в других помещениях, на другой территории;

2) соблюдением мер физической защиты резервных копий;

3) строгой регламентацией порядка использования резервных копий.

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

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

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

- немедленная реакция ответственного персонала.
- в дневное время суток сотрудник, обнаруживший внештатную (кризисную) ситуацию, должен поставить в известность диспетчера здания, непосредственного руководителя структурного подразделения, сотрудника Департамента по хозяйственной части (далее-ДХЧ), ответственного за контрольно-пропускную систему (далее – охрана) – устно, Центра Цифровизации– устно, при необходимости письменно;
- в ночное время суток, при возникновении внештатной ситуации, диспетчер должен поставить в известность пожарную службу, центральный пост полиции, в срочном порядке средствами телефонной связи оповещает ответственных руководителей Университета. Событие в обязательном порядке регистрируется в журнале дежурств, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных руководителей структурных подразделений, описание действий, направленных на устранение кризисной ситуации. По окончанию смены письменно ставится в известность Центр Цифровизации о случившейся кризисной ситуации.

2. Организацию работ и действий в кризисных ситуациях осуществляет ОИТП.

3. Контроль за организацией работ в кризисных ситуациях осуществляет Центр Цифровизации.

Наименование информационной системы	Где размещается ИС (Адрес, каб.№)	Вид резервного копирования (период возобновляемого копирования)	Ответственный за резервное копирование и порядок создания резервной копии (используемые технические средства)	Где хранится резервная копия (ответственный, его телефон)	Порядок использования резервной копии (кто, в каких случаях)

?????????? 2

Наименование основного технического средства	Наименование резервного технического средства	Вид резерва (групповой или индивидуальный, холодный или горячий), время готовности резерва	Ответственный за готовность резервного средства (период проверки работоспособности резервного средства)	Порядок использования (включения, настройки) резерва (для различных кризисных ситуаций)	Месторасположение резервного технического средства (ответственный, его телефон)

Кризисные ситуации

1. Отказ кондиционера воздуха

Температура помещения, в котором находятся компьютеры, не должна превышать 25 градусов, в противном случае принимаются следующие меры.

1) Сообщить СА ОИТП об инциденте с тем, чтобы он предпринял следующие действия:

- Корректно отключить сервера и источники бесперебойного питания.
- Он также уведомит Администраторов баз данных и программного обеспечения (Администраторов БД и ПО), с целью их привлечения к отключению системы.
- Сообщит своему руководству о данном инциденте.

2. Процедуры в случае пожарной тревоги

1) Сотрудник ОИТП должен сообщить об инциденте заведующему ОИТП, который предпримает следующие действия:

- Немедленно сообщает об инциденте Директору хозяйственного департамента.
- Директор хозяйственного департамента обязан обеспечить отключение рубильника (автомата) электрического питания.
- Попытаться погасить пожар ручным огнетушителем.
- Немедленно выключить сервера, телекоммуникационное оборудование, источники бесперебойного питания.
- Попытаться перенести используемые носители информации из помещения, в котором находятся сервера, в безопасное место.

Если не удается погасить пожар:

- Включите сигнал пожарной тревоги или вызовите пожарную службу по телефону 101(чрезвычайный вызов).

- Выходя из помещения, в котором находятся сервера, выключите аварийный выключатель электрического питания, расположенный рядом с дверью этого помещения.

Примечание: огнетушитель должен быть установлен на стене рядом с дверью в помещение, в котором находятся сервера. Действия, описанные в данном разделе необходимо производить, если серверное помещение не оборудовано средствами противопожарной безопасности и есть время на их выполнение (нет открытого огня и сплошного задымления), в противном случае данные действия квалифицируются как нарушение инструкции по противопожарной безопасности.

3. Процедуры при отказе электропитания

Если в серверном помещении появились проблемы с электрическим питанием, необходимо выполнить следующие шаги.

Сотрудник ОИТП должен сообщить об инциденте заведующему ОИТП, который предпринимает следующие действия:

- Немедленно сообщает об инциденте Директору хозяйственного департамента.
- Директор хозяйственного департамента обязан обеспечить отключение рубильника (автомата) электрического питания.
- Корректно отключить сервера и источники бесперебойного питания.

Он также уведомит Администраторов баз данных и программного обеспечения (Администраторов БД и ПО), с целью их привлечения к отключению системы.

4. Процедуры в случае затопления.

Если в серверном помещении появились проблемы связанные с затоплением серверного помещения, необходимо выполнить следующие шаги.

1) Сотрудник ОИТП должен сообщить об инциденте заведующему ОИТП, чтобы он предпринял следующие действия:

- Немедленно сообщил об инциденте Директору хозяйственного департамента.
- Директор хозяйственного департамента, должен обеспечить выключичение рубильника(автомат) электрического питания.
- Немедленно отключил сервера, телекоммуникационное оборудование.

Примечание: Ответственные специалисты ОИТП должны осмотреть оборудование для определения ущерба от поступления воды прежде, чем оно будет включено снова.

Revision #1
Created 2026-01-23 10:53:11 UTC by Ibrahim Tuncer
Updated 2026-01-23 10:57:35 UTC by Ibrahim Tuncer