Утверждаю :
Заведующий МБДОУ
д/с №11 «Радость»
Р.В. Чернецова
01.09.2016г.

Инструкция пользователя по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах МБДОУ №11 «Радость».

1. Общие положения

1.1 Настоящая инструкция разработана в соответствии с требованиями:
- Федерального закона от 27.07.2006 No152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №о1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. No21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных систем»

Инструкция пользователя по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах МБДОУ №11 «Радость».

1.2 Данная инструкция определяет порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее - ИС) МБДОУ №11 «Радость и по реагированию на нештатные ситуации, связанные с работой в ИС.

1.3 Пользователем ИС (далее - Пользователь) является сотрудник МБДОУ № 11 «Радость».участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС для выполнения своих должностных обязанностей.

1.4 Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими , организационно-распорядительными документами по вопросам информационной безопасности.

1.5 Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Общий порядок действий при возникновении нештатных ситуаций

2.1.

В настоящем документе под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а также с вероятностью потери защищаемой информации.

2.2. К нештатным ситуациям относятся следующие ситуации:
сбой в работе программного обеспечения («зависание»компьютера, медленная скорость работы программы, ошибки в работ программы и т. п.);
- отключение электричества;сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные - данные, отсутствие связи с сервером, повреждение файлов и т. п.);
- обнаружен вирус;
- обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);

- взлом системы (\уеЪ-сервера, файл-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);
- компрометация ключей (утеря носителя ключевой информации (Клйокеп, Е-1океп и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);
- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);
- физическое повреждение ЛВС или ПЭВМ (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИС и возможность потери защищаемой информации, и названные таковыми пользователем ИС или администратором безопасности информационных систем (далее Администратор безопасности ИС).

2.3. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность Единую диспетчерскую службу (далее - ЕДС) по телефону 8(3462)206939.

2.4. Специалисты ЕДС при выполнении заявки проводят предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководителя МБДОУ № 11 «Радость». Здесь и далее - все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет Пользователь, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС для выполнения своих должностных обязанностей.

2.5. По факту возникновения и устранения нештатной ситуации Пользователь заносит запись в «Журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах» МБДОУ № 11 «Радость».

2.6. Место хранения «Журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах» - кабинет руководителя МБДОУ №11 «Радость»

2.7. При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

3. Особенности действий при возникновении наиболее распространенных нештатных ситуаций.

3.1. Сбой программного обеспечения. Администратор безопасности ИС совместно с сотрудником отдела, у которого произошла нештатная ситуация, выясняют причину сбоя, направляют разработчику ПО информационное письмо с сопроводительными материалами о возникшей ситуации.
3.2. Отключение электричества. Администратор безопасности ИС совместно с Пользователем, у которого произошла нештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и ПО, а также проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.
3.3. Сбой в локальной вычислительной сети (далее - ЛВС). Пользователь проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, делает заявку в ЕДС на восстановление ПО и данных из последней резервной копии.
3.4. Выход из строя сервера. Администратор безопасности ИС, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы МБДОУ№11 «Радость». При необходимости осуществляется заявка в ЕДС по восстановлению ПО и данных из резервных копий.
3.5. Потеря данных. При обнаружении потери данных Пользователь делает заявку в ЕДС на поиск и устранение причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.), при необходимости, на восстановление ПО и данных из резервных копий.
3.6. Обнаружен вирус. При обнаружении вируса, Пользователь производит локализацию вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и сделать заявку в ЕДС для проведения анализа состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса Администратор безопасности ИС делает заявку в ЕДС для проведения внеочередной антивирусной проверки на всех ЭВМ МБДОУ №11 «Радость» с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных
копий. Проводится служебное расследование по факту появления вируса в .7. Обнаружена утечка информации. При обнаружении утечки информации ставится в известность Администратор безопасности ИС.
Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

3.8. Взлом системы ("УеЬ-сервера, файл-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера ставится в известность Администратор безопасности ИС. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Администратор безопасности ИС делает заявку в ЕДС на проверку целостности исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также на проведение анализасостояния файлов-скриптов и журналов сервера. Производится смена всех паролей, которые имели отношение к данному серверу. В случаенеобходимости специалистами ЕДС производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС МБДОУ № 11«Радость» после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование.

3.9. Попытка несанкционированного доступа (НСД). При обнаружении утечки информации ставится в известность Администратор безопасности ИС. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа). По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

3.10. Компрометация ключей. При обнаружении утечки информации ставится в известность Администратор безопасности ИС. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

3.11.Компрометация пароля. При обнаружении утечки информации ставится в известность Администратор безопасности ИС. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.). При необходимости, проводится служебное расследование.

3.12.Физическое повреждение ЛВС или ПЭВМ. Ставится в известность Администратор безопасности ИС. Определяется причина повреждения ЛВС или ПЭВМ. Администратор безопасности ИС делает заявку в ЕДС для определения возможных угроз безопасности , информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

3.13.Стихийное бедствие. При возникновении стихийных бедствий следует

руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в МБДОУ№11 «Радость»

4. Меры против возникновения нештатных ситуаций.

4.1. Администратором безопасности ИС периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

4.2. В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов и инструкций по эксплуатации оборудования и ПО.

4.3. Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

- Сбой программного обеспечения - применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.).
- Отключение электричества - использовать источники бесперебойного питания на критически важных технологических участках.
- Сбой ЛВС - обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем.
- Выход из строя серверов - применять надежные программно технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов.
- Потеря данных - периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администратором безопасности ИС (и сотрудниками) разъяснительные и обучающие собрания.
Обеспечить резервное копирование данных.
- Обнаружение вируса - соблюдать требования «Инструкции по организации антивирусной защиты».
- Утечка информации - применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации.
- Попытка несанкционированного доступа (НСД) - по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением Администратора безопасности ИС о попытках НСД.
- Компрометация паролей - соблюдать требования «Инструкции по организации парольной защиты».
- Физическое повреждение ЛВС или ПЭВМ - физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.
- Стихийное бедствие - проводить обучающие собрания и тренировки персонала МБДОУ№11 «Радость» по вопросам гражданской обороны.