Утверждено
приказом директора МБОУ СОШ с.Леонидово
№ 27 от 2.02.2015г.

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных
« Сетевой город.Образование» по обеспечению безопасности
при возникновении внештатных ситуаций

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет действия пользователей информационной системы персональных данных в случае возникновения внештатных ситуаций в процессах обработки персональных данных в информационных системах персональных данных (ИСПДн)
1.2. Положения инструкции обязательны для исполнения всеми должностными лицами в части выполнения вмененных им обязанностей.
1.3. Общими требованиями ко всем работникам школы в случае возникновения внештатной ситуации являются:
- работник, обнаруживший внештатную ситуацию, немедленно ставит в известность своего непосредственного руководителя и администратора информационной безопасности;
- администратор информационной безопасности (далее - администратор безопасности) обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководство Управления образования Поронайского городского округа. Кроме этого, администратор безопасности для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн , а также уполномоченного работника, ответственного за сопровождение технических средств ИСПДн;
- по факту возникновения внештатной ситуации и выяснению причин ее проявления проводится служебное расследование.

2. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДН ПРИ ВОЗНИКНОВЕНИИ ВНЕШТАТНЫХ СИТУАЦИЙ

2.1. Сбой программного обеспечения.
2.1.1. Администратор безопасности совместно с координатором СГО (далее - подразделение информационных технологий (ИТ)) выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения информационной безопасности (далее - подразделение информационной безопасности (ИБ) для принятия решения по существу.
2.2. Отключение электропитания технических средств ИСПДн.
2.2.1. Администратор безопасности совместно с уполномоченным работником подразделения ИТ проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.

2.3. Выход из строя технических средств ИСПДн (серверов).
2.3.1. Уполномоченный работник подразделения ИТ совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн .
2.3.2. О выходе из строя сервера уполномоченный работник подразделения ИТ, ответственный за эксплуатацию сервера , сообщает руководителю подразделения ИТ.
2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.
2.4. Потеря данных.
2.4.1. При обнаружении потери данных уполномоченный работник подразделения ИТ проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).
2.4.2. При необходимости уполномоченным работником подразделения ИТ производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте уполномоченный работник подразделения ИТ сообщает администратору безопасности. Администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.
2.5. Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн .
2.5.1. При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженный сервер физически отсоединяется от локальной вычислительной сети, и уполномоченным администратором безопасности проводится анализ состояния сервера.
2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки сервера данные могут быть потеряны. После успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.
2.5.3. После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.
2.5.4. По факту появления ВП в локальной вычислительной сети проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем подразделения ИБ.
2.6. Утечка информации.
2.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и координатор. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.
2.7. Взлом операционной системы средств автоматизации ИСПДн (несанкционированное получение доступа к ресурсам операционной системы).
2.7.1. При обнаружении взлома сервера ставится в известность руководитель подразделения ИТ и руководитель подразделения ИБ.
2.7.2. По возможности производится временное отключение сервера от локальной вычислительной сети для проверки на наличие ВП. Возможен временный переход на резервный сервер.

2.7.3. Уполномоченным работником подразделения ИТ проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Уполномоченным работником подразделения ИТ проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.
2.7.4. В случае необходимости уполномоченным работником подразделения ИТ производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.
2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн.
2.8. Попытка несанкционированного доступа (НСД).
2.8.1. При попытке НСД уполномоченным работником подразделения ИТ и администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.
2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, уполномоченным работником подразделения ИТ устанавливаются такие обновления.
2.8.3. По факту попытки НСД проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем подразделения ИБ.
2.8.4. В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.
2.9. Компрометация ключевой информации (паролей доступа).
2.9.1. При компрометации ключевой информации (пароля доступа) администратором безопасности проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.
2.9.2. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.
2.10. Физическое повреждение или хищение оборудования технических средств ИСПДн.
2.10.1. Работником, обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность: непосредственный руководитель, руководители подразделений ИБ и ИТ.
2.10.2. Уполномоченным работником подразделения ИТ совместно с администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности.
2.10.3. О факте повреждения элементов ИСПДн работник подразделения ИТ докладывает руководителю подразделения ИТ.
2.10.4. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.
2.10.5. Уполномоченным работником подразделения ИТ проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.6. При необходимости уполномоченным работником подразделений ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.
2.11. Невыполнение установленных правил ИБ (правил работы в ИСПДн), использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.
2.11.1. Работником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность: непосредственный руководитель и руководитель подразделения ИБ.
2.11.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.
2.11.3. Об обнаруженном факте администратор безопасности докладывает руководителю подразделения ИБ.
2.11.4. При необходимости по решению руководителя подразделения ИБ по фактам выявленных нарушений проводится служебное расследование.
2.12. Ошибки работников.
2.12.1. В случае возникновения сбоя, связанного с ошибками работников, руководитель подразделения , в котором произошел инцидент, ставит в известность уполномоченного работника подразделения ИТ и руководителя подразделения ИБ.
2.12.2. Администратором безопасности и уполномоченным работником подразделения ИТ проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.
2.12.3. При необходимости уполномоченным работником подразделения ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.
2.12.4. В случае нанесения значительного ущерба вследствие ошибок работников проводится служебное расследование.
2.13. Отказ в обслуживании.
2.13.1. Работником, обнаружившим отказ в обслуживании, ставятся в известность: непосредственный руководитель и руководители подразделений ИТ и ИБ.
2.13.2. Уполномоченным работником подразделения ИТ и администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.
2.13.3. Уполномоченным работником подразделения ИТ проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.
2.13.4. При необходимости, уполномоченным работником подразделения ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.
2.13.5. О причинах инцидента и принятых мерах уполномоченный работник подразделения ИТ информирует руководителя подразделения ИБ.
2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн.
2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.
2.14.2. Уполномоченным работником проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте администратор безопасности докладывает руководителю подразделения ИБ.
2.15. Техногенные и природные проявления внештатных ситуаций.
2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), работнику, обнаружившему факт возникновения нештатной ситуации:
- немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему непосредственному руководителю и администратору безопасности.
2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.
2.15.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.