

МКОУ «Варгашинская средняя школа №1»

ПРИКАЗ

28.12.2019 г.

№ 224 – ОД

Об утверждении инструкции по обеспечению безопасности персональных данных при возникновении внештатных ситуаций

В целях исполнения законодательных требований и реализации мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по обеспечению безопасности персональных данных при возникновении внештатных ситуаций в МКОУ «Варгашинская средняя школа № 1» (Приложение № 1).
2. Контроль за исполнением требований настоящего приказа оставляю за собой.



М.В. Колбина

ИНСТРУКЦИЯ
по обеспечению безопасности персональных данных при возникновении
внештатных ситуаций в МКОУ «Варгашинская средняя школа № 1»

I. Общие положения

- 1.1. Настоящая инструкция определяет действия работников Муниципального казенного общеобразовательного учреждения «Варгашинская средняя общеобразовательная школы № 1» (Далее - ОУ) в случае возникновения внештатных ситуаций в процессах обработки персональных данных в информационной системе.
- 1.2. Положения инструкции обязательны для исполнения всеми должностными лицами ОУ в части выполнения вмененных им обязанностей.
- 1.3. Общими требованиями ко всем работникам ОУ, в случае возникновения внештатной ситуации являются:
 - работник, обнаруживший внештатную ситуацию, немедленно ставит в известность ответственного за обработку персональных данных;
 - по факту возникновения внештатной ситуации и выяснению причин ее проявления проводится служебное расследование.

II. Действия пользователей информационной системы
при возникновении внештатных ситуаций

2.1. Сбой программного обеспечения

2.1.1. Ответственный за обработку персональных данных совместно с администратором информационной системы выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультации с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а так же файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте ответственный за обработку персональных данных сообщает директору ОУ для принятия решения.

2.2. Отключение электропитания технических средств информационной системы

2.2.1. Ответственный за обработку персональных данных совместно с администратором информационной системы 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 ответственный за обработку персональных данных сообщает директору ОУ для принятия решения.

2.3. Выход из строя технических средств информационной системы

2.3.1. Ответственный за обработку персональных данных совместно с администратором информационной системы выполняют мероприятия по немедленному вводу в действие резервной рабочей станции для обеспечения непрерывной работы информационной системы.

2.3.2. О выходе из строя рабочей станции ответственный за эксплуатацию рабочей станции сообщает ответственному за обработку персональных данных

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте ответственный за обработку персональных данных сообщает директору ОУ для принятия решения.

2.4. Потеря данных

2.4.1. При обнаружении потери данных администратор информационной системы 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 администратором информационной системы производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте ответственный за обработку персональных данных сообщает директору ОУ для принятия решения.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации информационной системы

2.5.1. При обнаружении вредоносной программы (ВП) производится её локализация с целью предотвращения её дальнейшего распространения. администратором информационной системы и ответственным за обработку персональных данных проводится анализ состояния рабочей станции.

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции данные могут быть потеряны. После успешной ликвидации ВП сохранённые 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 информационной системы и машинных носителях информации, с применением обновлённых 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 директором ОУ.

2.6. Утечка информации

2.6.1. При обнаружении утечки информации ставится в известность ответственный за обработку персональных данных. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищённости процессов информационной системы и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации информационной системы (несанкционированное получение доступа к ресурсам операционной системы)

2.7.1. При обнаружении взлома рабочей станции ставится в известность директор ОУ.

2.7.2. По возможности производится временное отключение рабочей станции. Возможен временный переход на резервную рабочую станцию.

2.7.3. Администратором информационной системы проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения.

Администратором информационной системы проводится анализ состояния файлов - скриптов и журналов, производится смена всех паролей, которые имели отношение к данной рабочей станции.

2.7.4. В случае необходимости Администратором информационной системы 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 рабочую станцию.

2.8. Попытка несанкционированного доступа (НСД)

2.8.1. При попытке НСД, администратором информационной системы и ответственным за обработку персональных данных 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, администратором информационной системы устанавливаются такие обновления.

2.8.3. По факту попытки НСД проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается директором ОУ.

2.8.4. В случае установления в ходе служебного расследования факта, осуществления попытки НСД со стороны внешних по отношению к информационной системе 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) ответственным за обработку персональных данных проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесённого) ущерба.

2.9.2. О произошедшем инциденте ответственный за обработку персональных данных сообщает директору ОУ для принятия решения.

2.10. Физическое повреждение или хищение оборудования технических средств информационной системы

2.10.1. Работником, обнаружившим физическое повреждение элементов информационной системы, ставится в известность ответственный за обработку персональных данных. Администратором информационной системы совместно с ответственным за обработку персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов информационной системы и возможные угрозы информационной безопасности.

2.10.2. О факте повреждения элементов информационной системы ответственный за обработку персональных данных докладывает директору ОУ.

2.10.3. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

2.10.5. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.6. При необходимости администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Невыполнение установленных правил информационной безопасности (правил работы в информационной системе), использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации

2.11.1. Работником, обнаружившим невыполнение установленных правил информационной безопасности, использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставится в известность ответственный за обработку персональных данных.

2.11.2. Ответственным за обработку персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.11.3. Об обнаруженном факте ответственный за обработку персональных данных докладывает директору ОУ.

2.11.4. При необходимости по решению директора ОУ по фактам выявленных нарушений проводится служебное расследование.

2.12. Ошибки пользователей

2.12.1. В случае возникновения сбоя, связанного с ошибками пользователей, руководитель структурного подразделения ОУ, в котором произошёл инцидент, ставит в известность инциденте ответственного за обработку персональных данных и администратора информационной системы.

2.12.2. Ответственный за обработку персональных данных совместно с администратором информационной системы проводят 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 администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.12.4. В случае нанесения ОУ значительного ущерба вследствие ошибок пользователей, проводится служебное расследование.

2.13. Отказ в обслуживании

2.13.1. Пользователем, обнаружившим отказ в обслуживании, ставится в известность ответственный за обработку персональных данных и администратор информационной системы. Администратором информационной системы и ответственным за обработку персональных данных проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.2. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах администратор информационной системы информирует ответственного за обработку персональных данных и директора ОУ.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) информационной системы

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) информационной системы ответственным за обработку персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.14.2. Администратором информационной системы 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 ответственный за обработку персональных данных докладывает директору ОУ.

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 внештатной 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 ответственному за обработку персональных данных.

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 уничтоженного оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбой общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка

14	Наводнение, вызванное проливным дождем
15	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
ИТ угрозы	
16	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
17	Ошибка персонала, имеющего доступ к серверу (рабочей станции)
18	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
19	Отключение электроэнергии
20	Сбой в работе интернет-провайдера
21	Физический разрыв внешних каналов связи