РАСПОРЯЖЕНИЕ

АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

15 июля 2019 г. г. Изобильный № 371-р

О мерах, направленных на реализацию постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

1. В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 18февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» утвердить:

1.1. Инструкцию пользователя по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах администрации Изобильненского городского округа Ставропольского края, согласно приложению 1.

1.2. Журнал учета нештатных ситуаций информационных систем, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах информационных систем администрации Изобильненского городского округа Ставропольского края, согласно приложению 2.

2. Контроль за выполнением настоящего распоряжения оставляю за собой.

3. Настоящее распоряжение вступает в силу со дня его подписания.

Глава Изобильненского городского округа Ставропольского края В.И. Козлов

АДМИНИСТРАЦИЯ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ
ОБЩИЙ ОТДЕЛ

Приложение 1

к распоряжению администрации
Изобильненского городского округа
Ставропольского края
от 15 июля 2019 г. № 371-р

ИНСТРУКЦИЯ
пользователя по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».

1.2. Данная инструкция определяет порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее – ИС) администрации Изобильненского городского округа Ставропольского края (далее – администрации) и по реагированию на нештатные ситуации, связанные с работой в ИС.

1.3. Пользователем ИС (далее – Пользователь) является сотрудник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС согласно приказу списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИС, для выполнения своих должностных обязанностей.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, 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, ошибки в работе 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 (web-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 (Rutoken, E-token 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 ИС.

2.3. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных (далее - администратор безопасности ИСПДн). В случае, если поставить в известность администратора не представляется возможным (администратор безопасности отсутствует на рабочем месте), пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

2.4. Администратор безопасности ИСПДн проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного начальника для определения дальнейших действий. Здесь и далее – в случае отсутствия администратора безопасности, все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет сотрудник отдела, временно назначенный начальником отдела, либо сам начальник.

2.5. По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС администрации».

2.6. 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 ИСПДн совместно с сотрудником отдела, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, разработчику ПО направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

3.2. Отключение электричества. Администратор безопасности ИСПДн совместно с сотрудником отдела, 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 (ЛВС). Администратор безопасности ИСПДн проводит анализ на наличие потерь и (или) разрушения

данных и ПО. В случае необходимо- сти, производится восстановление ПО и данных из последней резервной копии.

3.4. Выход из строя сервера. Администратор безопасности ИСПДн, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы администрации. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

3.5. Потеря данных. При обнаружении потери данных Администратор безопасности ИСПДн проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

3.6. Обнаружен вирус. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ 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 необходимо провести внеочередную антивирусную проверку на всех ЭВМ администрации с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС).

3.7. Обнаружена утечка информации. При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн. 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 (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера ставится в известность Администратор безопасности ИСПДн. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянские закладки. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным

ПО, следует особенно тщательно про- верить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС администрации, 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 ИСПДн. 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 и начальник подразделения. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

3.11. Компрометация пароля. При обнаружении утечки информации ставится в известность Администратор безопасности и начальник отдела администрации. 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 ИСПДн. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы 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 учреждении.

4. Меры против возникновения нештатных ситуаций

4.1. Администратором безопасности ИСПДн 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 Администрации;

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 администраторами информационной безопасности (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 информационной безопасности 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 администрации по вопросам гражданской обороны.

Приложение 2

к распоряжению администрации
Изобильненского городского округа
Ставропольского края
от 15 июля 2019 г. № 371-р

ЖУРНАЛ УЧЕТА
нештатных ситуаций информационных систем, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах информационных систем администрации Изобильненского городского округа Ставропольского края

№ п/п	Дата, ИСПДн, ПЭВМ, описание ситуации, выполненные работы	Подпись исполнителя	Подпись администратора
1.			
2.			
3.			
4.			
5.			