Приложение № 8
к приказу Комитета по внешним
связям Санкт-Петербурга
от 27.01.2015 № 1-П

ИНСТРУКЦИЯ
о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций в Комитете по внешним связям Санкт-Петербурга

1. Общие положения

1.1. Настоящая инструкция определяет действия государственных гражданских служащих (далее – сотрудники) и работников, замещающих должности, не являющиеся должностями государственной гражданской службы (далее – работники) Комитета по внешним связям Санкт-Петербурга (далее – Комитет) в случае возникновения нештатных ситуаций в процессе обработки персональных данных в информационных системах персональных данных (далее – ИСПДн).

1.2. Положения инструкции обязательны для исполнения всеми сотрудниками (работниками) в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем сотрудникам (работникам) в случае возникновения нештатной ситуации являются:

сотрудник (работник), обнаруживший нештатную ситуацию, немедленно ставит в известность руководителя структурного подразделения Комитета и администратора информационной безопасности;

администратор безопасности анализирует ситуацию, и в случае невозможности исправить положение, информирует службу технической поддержки Санкт-Петербургского государственного унитарного предприятия «Санкт-Петербургский информационно-аналитический центр» (далее – служба технической поддержки) об обнаружении нештатной ситуации в целях ее устранения;

администратор безопасности по факту возникновения нештатной ситуации представляет доклад председателю Комитета, по решению которого проводится служебная проверка в целях выяснения причин ее проявления.

2. Действие пользователей ИСПДн при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения.

2.1.1. Администратор безопасности совместно с уполномоченным сотрудником службы технической поддержки (далее – уполномоченный

сотрудник) выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами 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 для принятия решения по существу.

2.2. Отключение электропитания технических средств ИСПДн.

2.2.1. Администратор безопасности совместно с уполномоченным сотрудником 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 для принятия решения по существу.

2.3. Выход из строя технических средств ИСПДн (серверов, рабочих станций).

2.3.1. Уполномоченный сотрудник совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн (замене нерабочей станции).

2.3.2. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.3.3. О выходе из строя сервера (рабочей станции) администратор безопасности сообщает руководителю для принятия решения по существу.

2.4. Потеря данных.

2.4.1. При обнаружении потери данных уполномоченный сотрудник 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 сотрудником производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте уполномоченный сотрудник сообщает администратору безопасности. Администратор безопасности сообщает руководителю для принятия решения по существу.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн.

2.5.1. При обнаружении вредоносной программы (далее - ВП) уполномоченным сотрудником производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, проводится анализ состояния рабочей станции.

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции (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.

2.6. Утечка информации.

2.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и руководитель структурного подразделения. По факту инициируется процедура служебной проверки. 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. Компрометация ключевой информации (паролей доступа).

2.7.1. При компрометации ключевой информации (пароля доступа) уполномоченным сотрудником проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.7.2. О произошедшем инциденте администратор безопасности докладывает руководителю для принятия решения по существу.

2.8. Физическое повреждение или хищение оборудования технических средств ИСПДн.

2.8.1. Сотрудником, обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность непосредственный руководитель и администратор безопасности.

2.8.2. Уполномоченным сотрудником совместно с администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности.

2.8.3. О факте повреждения элементов ИСПДн администратор безопасности докладывает руководителю для принятия решения по существу.

2.8.4. Уполномоченным сотрудником проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.8.5. При необходимости уполномоченным сотрудником проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

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

2.9.1. Сотрудником (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 администратор безопасности.

2.9.2. Уполномоченным сотрудником и администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности (далее – ИБ) в результате инцидента.

2.9.3. Об обнаруженном факте администратор безопасности докладывает руководителю.

2.10. Ошибки сотрудников (работников).

2.10.1. В случае возникновения сбоя, связанного с ошибками сотрудников (работником), руководитель подразделения Комитета, в котором произошел инцидент, ставит в известность уполномоченного сотрудника и администратора безопасности.

2.10.2. Администратором безопасности и уполномоченным сотрудником 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.

2.10.3. При необходимости уполномоченным сотрудником проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Отказ в обслуживании.

2.11.1. Сотрудником, обнаружившим отказ в обслуживании, ставятся в известность непосредственный руководитель и уполномоченный сотрудник.

2.11.2. Уполномоченный сотрудник проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.11.3. Уполномоченным сотрудником проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.11.4. При необходимости, уполномоченным сотрудником проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11.5. О причинах инцидента и принятых мерах уполномоченный сотрудник информирует администратора безопасности.

2.12. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн.

2.12.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн уполномоченным сотрудником и администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.12.2. Уполномоченным сотрудником проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.12.3. Об инциденте администратор безопасности докладывает руководителю.

2.13. Техногенные и природные проявления нештатных ситуаций.

2.13.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику (работнику), обнаружившему факт возникновения нештатной ситуации надлежит:

немедленно оповестить других сотрудников (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 руководителю структурного подразделения Комитета и администратору безопасности.

2.13.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.13.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.