Приложение №3
к приказу от «__» _____ 202_ №_____

УТВЕРЖДАЮ
Врио директора
ФГБУ «СибНИГМИ»
_____ В.Н. Копылов
«__» _____ 202_ г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах персональных данных ФГБУ «СибНИГМИ»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана в соответствии с требованиями:
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 № 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 - ИСПДн) и по реагированию на нештатные ситуации, связанные с работой в ИСПДн в ФГБУ «СибНИГМИ» (далее - Институт).

1.3. Пользователем ИСПДн (далее - Пользователь) является работник Института, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн согласно приказу списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИСПДн, 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 работников под личную подпись. Пользователь должен быть предупрежден о возможной ответственности за нарушение.

II . ОБЩИЙ ПОРЯДОК ДЕЙСТВИЙ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

- В настоящей Инструкции под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также с вероятностью потери защищаемой информации.
- К нештатным ситуациям относятся следующие ситуации:
- сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, 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.);
- обнаружение вируса;
- обнаружение утечки 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 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 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 учетной записи пользователя);
- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т.п.);
- физическое повреждение локально-вычислительной сети (далее - ЛВС) или персонального компьютера (далее - ПК) (не включается ПК, при попытке включения отображается синий или черный экран, повреждены провода и т.п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИСПДн и возможность потери защищаемой информации, и названные таковыми пользователем ИСПДн или ответственным за ИСПДн.
- При возникновении нештатных ситуаций во время работы, обнаруживший нештатную ситуацию, немедленно ставит в известность лицо, ответственное за техническую защиту информации в Институте (далее - ответственный за ИСПДн). В случае, если поставить в известность вышеуказанное лицо не представляется возможным, составляется служебная записка в произвольной форме с описанием нештатной ситуации, и передается ответственному за обработку персональных данных в Институте.
- Ответственный за ИСПДн проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного руководителя для определения дальнейших действий.
- По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИСПДн».
- При необходимости проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

III. ОСОБЕННОСТИ ДЕЙСТВИЙ ПРИ ВОЗНИКНОВЕНИИ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ НЕШТАТНЫХ СИТУАЦИЙ.

- Сбой программного обеспечения: ответственный за ИСПДн совместно с работником, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, сообщение о нештатной ситуации передается ответственному за обработку персональных данных в Институте.

- Отключение электричества: ответственный за ИСПДн и работник, у которого произошла нештатная ситуация, проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения (далее - ПО), а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.
- Сбой в локальной вычислительной сети: ответственный за ИСПДн проводит анализ на наличие потерь и (или) разрушение данных и ПО. В случае необходимости производится восстановление ПО и данных из последней резервной копии.
- Выход из строя сервера: ответственный за ИСПДн проводит меры по немедленному вводу в действие резервного сервера (при наличии) для обеспечения непрерывной работы пользователей ИСПДн. В случае необходимости производится восстановление ПО и данных из последней резервной копии.
- Потеря данных: при обнаружении потери данных, ответственный за 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 резервной копии.
Обнаружен вирус: 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 ответственным за ИСПДн. Результатом анализа может быть попытка сохранения (спасения) данных, т.к. 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 Регламентом настройки и эксплуатации системы антивирусной защиты. После ликвидации необходимо провести внеочередную антивирусную проверку на всех ЭВМ с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных данных из резервных копий. Проводится служебное расследование по факту появления вируса.

- Обнаружена утечка информации. При обнаружении утечки информации необходимо сообщить ответственному за ИСПДн, а также ответственному за обработку персональных данных в Институте. Провести служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновению.
- Взлом системы (Web-сервера и др.) или несанкционированный доступ (далее - НСД). При обнаружении взлома сервера 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 антивирусом ПО, следует особенно тщательно проверить 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, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование.
Попытка несанкционированного доступа. При обнаружении утечки информации необходимо поставить в известность ответственного за ИСПДн, а также ответственного за обработку персональных данных в Институте. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принять меры по предотвращения НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такое обновление.

- Компрометация ключей. При обнаружении утечки информации необходимо сообщить ответственному за ИСПДн. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.
- Компрометация пароля. При обнаружении утечки информации необходимо сообщить ответственному за ИСПДн, сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять меры по минимизации возможного (или нанесенного) ущерба. При необходимости провести служебное расследование.
- Физическое повреждение ЛВС или ПК. Необходимо сообщить ответственному за ИСПДн. Определить причины повреждения ЛВС или ПК и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод из строя оборудования провести служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Анализ электронных журналов. При необходимости провести меры по восстановлению ПО и данных из резервных копий.
- Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими действия при ЧС.

IV. МЕРЫ ПРОТИВ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ.

- Ответственным за ИСПДн не реже 1 раза в год должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.
- В общем случае, для предотвращения нештатных ситауций необходимо четкое соблюдение требований нормативных документов и инструкций по эксплуатации оборудования и ПО.
- Рекомендации по предотвращению некоторых типичных нештатных ситауций:
- 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 участках;
- сбой ЛВС - обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем;
- выход из строя серверов - применять надежные программнотехнические 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. Обеспечить резервное копирование данных;
- обнаружение вируса - соблюдать требования Регламента настройки и эксплуатации системы 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 - по возможности установить регистрацию попыток НСД на всех участках, где возможен несанкционированный доступ, с оповещением ответственного за ИСПДн о попытках НСД;
- компрометация паролей - соблюдать требования «Инструкции пользователя информационной системы персональных данных»;
- физическое повреждение ЛВС или ПК - физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним;
- стихийное бедствие - проводить обучающие собрания и тренировки работников по вопросам гражданской обороны.