СОГЛАСОВАНО:

Председатель профкома ИНЦ СО РАН

_____/С.А. Мазилкин

01 ноября 2019

УТВЕРЖДАЮ:

Директор ИНЦ СО РАН, д.м.н.

_____/ К.А. Апарцин

01 ноября 2019.

ИНСТРУКЦИЯ
работников ИНЦ СО РАН, допущенных к обработке конфиденциальной информации

г.Иркутск

1. Общие положения

1.1 Настоящая инструкция разработана в соответствии с требованиями:

– Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– «Требований к защите персональных данных при их обработке в информационных системах персональных данных» утвержденной постановлением Правительства Российской Федерации от 01.11.2012 №1119.

1.2 Данная инструкция определяет общие обязанности, права и ответственность пользователя информационных систем ИНЦ СО РАН по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.

1.3 Пользователем ИС (далее – Пользователь) является работник ИНЦ СО РАН, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС.

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. Обязанности пользователя

2.1 При выполнении работ в ИС Пользователь обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);

– хранить втайне свои идентификационные данные (имена, пароли и т. д.);

– выполнять требования, предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т. д.), осуществлять вход на АРМ только под своими идентификационными данными;

– передавать для хранения установленным порядком свое индивидуальное устройство идентификации, и другие реквизиты разграничения доступа, только руководителю своего подразделения или администратору безопасности ИС (ответственному за информационную безопасность подразделения);

– выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИС;

– немедленно вызывать администратора безопасности ИС и ставить в известность руководителя подразделения в случае утери индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ, ставить в известность администратора безопасности ИС при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

– работать в ИС только в разрешенный период времени;

– немедленно выполнять предписания администраторов безопасности ИС, предоставлять свое АРМ администратору безопасности для контроля;

– ставить в известность администраторов ИС в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т. п.), а также перебоев в системе электроснабжения;

– осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;

– уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;

– сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИС.

2.2 Пользователю категорически запрещается:

– использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

– самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИС (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;

– осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить конфиденциальную информацию на неучтенных носителях информации, в том числе для временного хранения;

– оставлять включенное без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);

– передавать кому-либо свое индивидуальное устройство идентификации в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы устройства идентификации;

– оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИС (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности ИС (ответственного за безопасность информации) и руководителя своего подразделения;

– подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;

– осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;

– фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;

– разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;

– вносить изменения в файлы, принадлежащие другим пользователям.

3. Права пользователя

3.1 Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;
- требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Правила работы в сетях общего доступа

4.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИС, должна производиться при служебной необходимости.

4.2 При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);
- передавать по Сети защищаемую информацию без использования средств защиты каналов связи;
- запрещается загружать из Сети программное обеспечение;
- запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);
- запрещается нецелевое использование подключения к сети.

5. Ответственность пользователя

5.1 Пользователь несет персональную ответственность за:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения.
- разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы.

5.2 Ответственность за нарушение функционирования ИС, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

5.3 Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами ИНЦ СО РАН (см. Приложение 1 к настоящей инструкции).

Приложение 1

Выдержки из статей Уголовного кодекса РФ, определяющие ответственность пользователей за нарушение установленных правил обработки информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Статья 293. Халатность

1. Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, - наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо

исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

2. То же деяние, повлекшее по неосторожности смерть человека или иные тяжкие последствия, наказывается лишением свободы на срок до пяти лет.