ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ НАУКИ

ИНСТИТУТ

МОЛЕКУЛЯРНОЙ И КЛЕТОЧНОЙ БИОЛОГИИ

СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК

П Р И К А З

23 сентября 2022 г. № 62

г. Новосибирск

Об утверждении инструкции
по организации безопасной работы
с информационной системой института

В целях повышения информационной безопасности института и во исполнение письма Управления ФСБ России по Новосибирской области от 21.09.2022 № 108/20/2750 «О направлении рекомендаций»

П Р И К А З Ы В А Ю:

1. Ввести в действие Инструкцию по организации безопасной работы с информационной системой Федерального государственного бюджетного учреждения науки Института молекулярной и клеточной биологии Сибирского отделения Российской академии наук (далее – Инструкция) (Приложение № 1).

2. Заместителю директора по общим вопросам Зыкову И.А. в срок до 28 сентября 2022 года организовать размещение Инструкции на официальном сайте Института.

3. Заместителю директора по общим вопросам Зыкову И.А. обеспечить незамедлительное ознакомление работников Института с Инструкцией.

4. Контроль исполнения настоящего приказа оставляю за собой.

Директор С.А. Демаков

Приложение № 1
к приказу от 23.09.2022 № 62

«УТВЕРЖДАЮ»
директор ИМКБ СО РАН

д.б.н. С.А. Демаков
«23» сентября 2022 г.

Инструкция
по организации безопасной работы с информационной системой
Федерального государственного бюджетного учреждения науки
Института молекулярной и клеточной биологии
Сибирского отделения Российской академии наук

1. Общие положения и область применения

1.1 Инструкция по организации безопасной работы с информационной системой (далее - инструкция) Федерального государственного бюджетного учреждения науки Института молекулярной и клеточной биологии Сибирского отделения Российской академии наук (далее – Институт) разработана на основании требований инструкций по эксплуатации технических и программных средств от производителя, Федерального закона «Об информации, информационных технологиях и о защите информации», Уголовного кодекса Российской Федерации.

1.2 Настоящая инструкция распространяется на все виды работ на персональных электронно-вычислительных машинах (далее - ПЭВМ или компьютер), копировальном оборудовании, регламентирует правила использования защищаемой информации баз данных, порядок допуска пользователей ПЭВМ к работе в составе локальной вычислительной сети (ЛВС).

1.3 Положения инструкции обязательны для исполнения всеми работниками-пользователями ПЭВМ, ЛВС Института.

1.4 Ответственность за выполнение требований настоящей инструкции возлагается на руководителей подразделений.

2. Технические средства и стандартизация программного обеспечения

2.1 Технические средства включают аппаратные и программные средства. Аппаратные средства - это материальные объекты. В данной инструкции рассматриваются ПЭВМ, серверное и коммуникационное оборудование компьютерной сети. Программные средства - это системное программное обеспечение прикладные программы, а также средства экранного и печатного представления - пользовательский интерфейс. Это нематериальные объекты.

2.2 Технические средства предоставляют различный уровень защиты от несанкционированного доступа и случайных сбоев и обладают различными возможностями. Регламентирование работы с техническими средствами это установление правил, обеспечивающих эффективность работы, необходимую безопасность и защиту информации с учетом этих факторов.

2.3 Системный администратор, обслуживающий информационные системы производит установку только лицензионного программного обеспечения (ПО).

2.4 На всех серверах Института используются операционные системы (ОС) Linux, Windows, MacOS. На серверах, выполняющих специфические задачи, не позволяющие использовать указанные ОС, допускается установка других ОС. Необходимость установки ОС отличной от указанной определяет администратор ЛВС и согласовывает с директором.

2.5 На всех рабочих станциях используются ОС Linux, Windows, MacOS. Установка других операционных систем допускается в следующих случаях:

- аппаратная конфигурация рабочей станции не отвечает минимальным требованиям ОС Linux, Windows, MacOS;
- программное обеспечение, необходимое пользователю для выполнения должностных обязанностей не совместимо с ОС Linux, Windows, MacOS. В этом случае решение об установке иной версии операционной системы определяет администратор ЛВС и согласовывает с директором.

2.6 Первоначальная установка оборудования, установка дополнительных устройств, ремонт, техническое обслуживание и первоначальное конфигурирование операционной системы рабочей станции компьютерной сети Института производится системным администратором, обслуживающим информационную систему. Установка, переустановка, изменение ключевых параметров операционной системы пользователем недопустима.

2.7 Установка и первоначальное конфигурирование операционной системы на сервере производится системным администратором, обслуживающим информационные системы Института. Установка и изменение параметров сервера другими работниками Института недопустима.

2.8 Настройка принтеров для коллективного пользования в компьютерной сети производится системным администратором, обслуживающим информационную систему.

3. Правила регистрации пользователей ПЭВМ в ЛВС и наделение их полномочиями доступа к ресурсам информационной системы Института

3.1 С целью соблюдения персональной ответственности за свои действия каждому работнику-пользователю ПЭВМ, допущенному к работе в ЛВС, присвоено персональное уникальное имя (учетная запись пользователя), под которым он регистрируется и работает в сети. Использование несколькими работниками при работе в ЛВС одного и того же имени пользователя («группового имени») запрещается.

3.2 Процедура регистрации пользователя для работников Института и предоставления ему (или изменения его) прав доступа к ресурсам информационной системы инициируется заявкой руководителя подразделения, в которой работает данный работник.

3.3 В заявке указывается: содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам информационной системы ранее зарегистрированного пользователя, использование сетевого принтера для печати документов);

- должность (с полным наименованием подразделения), фамилия, имя и отчество работника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных рабочих станциях компьютерной сети);
- срок начала и окончания действия доступа.

3.4 Заявку визирует директор, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к необходимым для решения им указанных задач ресурсам информационной системы.

3.5 системный администратор рассматривает представленную заявку вносит необходимые изменения в списки пользователей.

3.6 На основании заявки системный администратор производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к сетевым ресурсам ЛВС, включению его в соответствующие задачам группы пользователей и другие необходимые действия.

3.7 По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью системного администратора.

3.8 Работнику, зарегистрированному в качестве нового пользователя системы, под роспись сообщается имя соответствующего ему пользователя, выдается начальное значение пароля, которое он обязан сменить при первом же входе в систему.

3.9 Подключение пользователей к сети Интернет производится по заявке руководителя структурного подразделения, подписанной директором.

3.10 Исполненные заявки хранятся у системного администратора и могут впоследствии использоваться для восстановления учетных записей и полномочий пользователей после аварий, контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам информационной системы при разборе конфликтных ситуаций.

4. Правила организации парольной защиты информационной системы Института

4.1 Личные пароли выбираются пользователями компьютерной сети самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- среди символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому;
- смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

4.2 Внеплановая смена личного пароля или удаление учетной записи пользователя компьютерной сети в случае прекращения его полномочий (увольнение, переход на другую работу внутри Института и т.п.) должна производиться системным администратором после окончания последнего сеанса работы данного пользователя с системой, по заявке руководителя подразделения.

4.3 Внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Института и другие обстоятельства) системного администраторов и других

работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой информационной системы.

4.4 В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.4.2 или п.4.3 настоящей Инструкции, в зависимости от полномочий владельца скомпрометированного пароля.

4.5 Хранение пользователями ПЭВМ значений своих действующих паролей на бумажном носителе допускается только в опечатанном владельцем пароля сейфе, либо (для случаев возникновения нештатных ситуаций и необходимости из-за этого использования имен и паролей некоторых пользователей в их отсутствие, обязательно) в сейфе руководителя подразделения, в опечатанном владельцем пароля пенале или запечатанном конверте.

4.6 Повседневный контроль при работе пользователей информационной системы с паролями, соблюдением порядка их смены хранения и использования возлагается на руководителей подразделений, периодический контроль возлагается на системного администратора.

5. Правила организации антивирусной защиты

5.1 К использованию в информационной системе Института допускаются только лицензионные антивирусные средства, централизованно закупленные Институтом и рекомендованные к применению системным администратором.

5.2 Установка средств антивирусного контроля на компьютерах, серверах ЛВС Института осуществляется системным администратором в соответствии с руководствами по применению конкретных антивирусных средств.

5.3 В начале работы при включении ПЭВМ (для серверов ЛВС - при перезапуске), а также при первом доступе к файлам в автоматическом режиме проводится их антивирусный контроль. Один раз в неделю, в автоматическом режиме производится полная проверка дисков ПЭВМ, подключенных к ЛВС, на наличие вирусов.

5.4 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере.

5.5 Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель). Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

5.6 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено системным администратором на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть также выполнена антивирусная проверка системным администратором.

5.7 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщение с системных ошибках и т.п.), пользователь ПЭВМ самостоятельно, или вместе системным администратором, должен провести внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

5.8 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ПЭВМ обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела технического обслуживания информационных систем);
- в случае обнаружения нового вируса, не распознанного установленными антивирусными средствами, привлечь системного администратора.

5.9 Периодический контроль состояния антивирусной защиты в компьютерной сети, соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей инструкции пользователями ПЭВМ подразделений Института, осуществляется системным администратором.

6. Защита информации при технических сбоях и попадании вирусных программ

6.1 Потеря информационных ресурсов при технических сбоях, проникновении в компьютерную сеть вредоносных или разрушительных программ может повлечь нарушения в работе Института.

6.2 Для сокращения времени на восстановление информационной системы из-за утраты данных по техническим причинам, вирусных атак или неверных

действий работников производится резервное копирование программных файлов, баз данных, каталогов.

6.3 Резервное копирование данных информационной системы осуществляется системным администратором ЛВС.

7. Ответственность пользователей информационной системы

7.1 Пользователи ПЭВМ и компьютерной сети за нарушение положений настоящей Инструкции несут административную и уголовную ответственность в соответствии с законодательством РФ.