

**Федеральное государственное бюджетное научное учреждение
«ФЕДЕРАЛЬНЫЙ НАУЧНЫЙ ЦЕНТР - ВСЕРОССИЙСКИЙ НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ЭКСПЕРИМЕНТАЛЬНОЙ ВЕТЕРИНАРИИ
ИМЕНИ К.И. СКРЯБИНА И Я.Р. КОВАЛЕНКО
РОССИЙСКОЙ АКАДЕМИИ НАУК»
(ФГБНУ ФНЦ ВИЭВ РАН)**

ПРИКАЗ

«15» марта 2022 г.

№ 22 -ОД

Москва

Об обеспечении кибербезопасности в ФГБНУ ФНЦ ВИЭВ РАН

В соответствии с письмом Минобрнауки России от 11.03.2022 № МН-19/275-АН, письмом Минобрнауки России от 14.03.2022 № МН-19/191, в целях организации взаимодействия учреждений по борьбе с киберугрозами

ПРИКАЗЫВАЮ:

1. Возложить на заместителя директора по общим вопросам, имущественным и земельным отношениям Ушакову Г.Г. ответственность за обеспечение кибербезопасности в ФГБНУ ФНЦ ВИЭВ РАН (далее – Центр). Обеспечить в прямом подчинении заместителя директора по общим вопросам, имущественным и земельным отношениям инженера по защите информации Горячева Павла Андреевича.

2. Отделу кадров при необходимости осуществить внесение соответствующих изменений в должностные инструкции и локальные акты Центра (отв. Захарова И.А.).

3. Руководителям филиалов назначить ответственных за обеспечение кибербезопасности и направить эти сведения в Центр.

4. В Центре и филиалах обеспечить мониторинг инцидентов в области кибербезопасности и их регистрацию (отв. Горячев П.А., руководители филиалов). Ответственным за обеспечение кибербезопасности в филиалах осуществлять взаимодействие с Центром.

5. В срок, указанный в письме от 11.03.2022 № МН-19/275-АН и по прилагаемым формам обеспечить своевременный сбор и передачу информации в Штаб Минобрнауки России по борьбе с киберугрозами (далее - Штаб) на адрес электронной почты: cyberthreats@minobrnauki.gov.ru, а также осуществлять дальнейшее взаимодействие со Штабом и сообщать о возникших инцидентах (отв. Ушакова Г.Г.).

6. В Центре и филиалах в целях минимизации рисков, связанных с использованием оборудования и программного обеспечения иностранного производства, задействованного в обеспечении информационной безопасности:

6.1. предпринять меры по ограничению использования оборудования и программного обеспечения иностранного производства в области защиты информации с учетом необходимости сохранения и повышения уровня защищенности информации.

6.2. принять меры по организации резервного копирования ключевых элементов информационной инфраструктуры, служебной и иной информации, необходимой для выполнения функций учреждения.

6.3. в случае использования в информационной инфраструктуре сертификатов безопасности, выпущенных в иностранных центрах сертификации, обеспечить использование сертификатов российских удостоверяющих центров.

7. В Центре и филиалах осуществить перечень мер по повышению защищенности публичных ресурсов, а именно:

7.1 проверить наличие доступа в личные кабинеты регистраторов доменных имен для публичных ресурсов в сети «интернет». в случае его отсутствия выполнить необходимые действия по восстановлению доступа.

7.2. обновить и (или) усложнить парольную политику, сменить пароли в личных кабинетах регистраторов доменных имен, пароли администраторов публичных ресурсов, а также, при наличии возможности, ввести дополнительные факторы аутентификации пользователей.

7.3. перейти на использование серверов dns, находящихся на территории российской федерации.

7.4. удалить из шаблонов страниц html весь код javascript, загружаемый с иностранных ресурсов (баннеры, счётчики и т.п.).

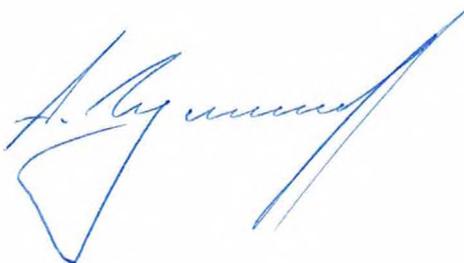
7.5. в случае использования иностранного хостинга переместить размещённые на нём публичные ресурсы на российский хостинг.

7.6. в случае размещения публичного ресурса в доменной зоне, отличной от доменной зоны '.ru', по возможности переместить его в доменную зону '.ru'.

8. Разместить настоящий Приказ на официальном сайте ФГБНУ ФНЦ ВИЭВ РАН (отв. Бочаров А.Е.).

9. Контроль исполнения настоящего приказа оставляю за собой.

Директор



А.М. Гулюкин