МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минобрнауки России)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРОБЛЕМ РЕГИОНАЛЬНОЙ ЭКОНОМИКИ РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИПРЭ РАН)

«17» марта 2022 г. Санкт-Петербург

ПРИКАЗ № 24

«О мерах по повышению защищенности информационной инфраструктуры ИПРЭ РАН»

В соответствии с письмом заместителя министра Минобрнауки России А.В. Нарукавникова №МН-19/257-АН от 04.03.2022г., МН-19/275-АН от 11.03.2022 г. и директора Департамента цифрового развития Минобрнауки России М.А. Сапунова № МН-19/143 от 09.03.2022 г. «О мерах по повышению защищенности информационной инфраструктуры РФ»

ПРИКАЗЫВАЮ:

1. С целью предотвращения получения хакерскими группировками информации об особенностях функционирования информационных систем Института проблем региональной экономики РАН принять дополнительные меры:

1.1. Проинформировать пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;

1.2. Проинформировать сотрудников ИПРЭ РАН – пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;

1.3. Усилить контроль над действиями пользователей информационных систем, используемых в ИПРЭ РАН;

1.4. Провести внеплановую смену паролей пользователей, используемых для доступа в информационные системы;

Ответственные:
Руководитель административного аппарата директора Костяновская Е.Б.,
Главный специалист по программному обеспечению Гузий Л.И.,
Помощник директора Тарасова О.А.

1.5. Рассылку официальных документов ИПРЭ РАН осуществлять с письменного разрешения директора Института;

1.6. Внутреннюю рассылку электронных писем сотрудникам ИПРЭ РАН осуществлять с электронной почты дирекции Института info@ireras.ru

2. Исключить автоматическое централизованное обновление посредством сети «Интернет» применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза.
3. Возложить ответственность за обеспечение кибербезопасности учреждения в рамках должностной инструкции на руководителя научного направления д.э.н., проф. Кузнецова С.В.
4. Обеспечить мониторинг инцидентов в области кибербезопасности и их регистрацию согласно Таблице 3 (Приложение).
   Ответственный:
   Главный специалист по ПО Гузий Л.И.
5. Обеспечить своевременную передачу информации о возникших инцидентах в Штаб Минобрнауки России по борьбе с киберугрозами.
   Ответственный:
   Главный специалист по ПО Гузий Л.И.
6. Направить в Штаб Минобрнауки России по борьбе с киберугрозами информацию о принятых мерах согласно п. 3-5.
   Ответственный:
   Главный специалист по ПО Гузий Л.И.
7. Направить в Штаб Минобрнауки России по борьбе с киберугрозами информацию об используемом оборудовании согласно Таблице 1 (Приложение) и используемом программном обеспечении согласно Таблице 2 (Приложение).
   Ответственный:
   Главный специалист по ПО Гузий Л.И.
8. Предпринять меры по ограничению использования оборудования и программного обеспечения иностранного производства в области защиты информации с учетом необходимости сохранения и повышения уровня защищенности информации.
   Ответственный:
   Главный специалист по ПО Гузий Л.И.
9. Принять меры по организации резервного копирования ключевых элементов информационной инфраструктуры, служебной и иной информации, необходимой для выполнения функций учреждения.
   Ответственный:
   Главный специалист по ПО Гузий Л.И.

10. В случае использования в информационной инфраструктуре учреждения сертификатов безопасности, выпущенных в иностранных центрах сертификации, обеспечить использование сертификатов российских удостоверяющих центров.
    Ответственный:
    Главный специалист по ПО Гузий Л.И.

11. Контроль за исполнением настоящего приказа оставляю за собой.

Директор ИПРЭ РАН А.Д. Шматко

Приложение
к приказу №24 от 17.03.2022 г.

Таблица 1.
«Оборудование иностранного производства, используемое в области защиты информации»

№	Наименование	Целевое предназначение устройства (например - коммутатор, межсетевой экран, криптографический шлюз и т.д.)	Страна происхождения (согласно паспорту устройства)	Дата ввода в эксплуатацию (дд.мм.гг.)	Количество (шт.) 1.

Таблица 2.
«Программное обеспечение иностранного производства, используемое в области защиты информации»

№	Наименование	Целевое предназначение устройства (например - межсетевой экран, SIEM и т.д.)	Страна происхождения	Год окончания действия лицензии на право использования (например – 2022 г., бессрочно)	Количество (шт.)

Таблица 3.
«Мониторинг инцидентов в области кибербезопасности»

№	Тип компьютерной атаки	Объект компьютерной атаки	Дата и время компьютерной атаки	Принятые меры по устранению последствий компьютерной атаки	Примечание