ИНТЕР РАО ЕЭС
энергия без границ

ПРИКАЗ

09.06.2022 ИРАО/232

Москва

Об исполнении поручения Оперативного штаба
по обеспечению устойчивого функционирования
компаний Группы «Интер РАО»

В целях реализации первоочередных мер по защите объектов информационной инфраструктуры Группы «Интер РАО», предусматривающих обеспечение целостности и общедоступности информации, и во исполнение поручений Указа Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250, Оперативного штаба Минэнерго России (п. 2 протокола от 10.03.2022 № НШ-54/1пр) и Оперативного штаба по обеспечению устойчивого функционирования компаний Группы «Интер РАО»

ПРИКАЗЫВАЮ:

1. Утвердить рекомендации по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий компаний Группы «Интер РАО» (далее – Рекомендации) в соответствии с приложением № 1 к настоящему приказу.
2. Руководителю Департамента информационной безопасности Чугунову А.В. организовать информирование единоличных исполнительных органов компаний Группы «Интер РАО» по списку в соответствии с приложением № 2 к настоящему приказу и работников, назначенных ими в рамках исполнения п. 2 Рекомендаций (далее – Исполнитель) о дополнительных рекомендациях на основании нормативно-правовых актов, указаний и рекомендаций органов государственной власти.
3. Единоличным исполнительным органам компаний Группы «Интер РАО» по списку в соответствии с приложением № 2 к настоящему приказу рекомендовать обеспечить реализацию Рекомендаций и размещение отчёта об исполнении Рекомендаций в отчёте в карточке резолюции настоящего приказа в АСУД.

Срок: в соответствии со сроком, определенным в Рекомендациях.

4. Единоличному исполнительному органу ООО «Интер РАО – Управление электрогенерацией» рекомендовать обеспечить выполнение в АО «Интер РАО - Электрогенерация», в ООО «КВАРЦ Групп» и АО «Нижневартовская ГРЭС» мероприятий, указанных в п. 3 настоящего приказа.

Срок: в соответствии со сроком, определённым в Рекомендациях.

5. Члену Правления – руководителю Финансово-экономического центра Мирошниченко Е.Н. обеспечить финансирование мероприятий, определенных приложением № 1 к настоящему приказу.

6. Контроль за исполнением настоящего приказа возложить на руководителя Департамента информационной безопасности Чугунова А.В.

Генеральный директор Б.Ю. Ковальчук

Рассылается: членам Оперативного штаба по обеспечению устойчивого функционирования компаний Группы «Интер РАО», Генеральным директорам компаний Группы «Интер РАО» в соответствии с приложением № 2 к настоящему приказу

Васильев Дмитрий Николаевич
26 05

Приложение № 1 к приказу
ПАО «Интер РАО»
от 09.06.2022 № ИРАО/232

Рекомендации
по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий компаний
Группы «Интер РАО»

Настоящие рекомендации по обеспечению информационной безопасности компаний Группы «Интер РАО» (далее – Рекомендации) определяют перечень организационных и технических мероприятий, реализацию которых рекомендуется осуществить компаниям Группы «Интер РАО» (далее - Компании) с целью противодействия компьютерным атакам.

В целях обеспечения необходимого уровня информационной безопасности в сфере информационно-коммуникационных технологий Компаниям рекомендуется:

1. Возложить на руководителя Компании персональную ответственность за обеспечение информационной безопасности Компании. В случае необходимости инициировать и обеспечить контроль реализации соответствующих корпоративных процедур.

Срок: 30.06.2022.

2. Возложить на лицо из числа заместителей руководителя Компании полномочия по обеспечению информационной безопасности Компании, а также обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в Компании (далее – ответственный по информационной безопасности). Ответственному по информационной безопасности проработать вопрос кадрового и материально-технического усиления подразделения Компании по информационной безопасности (далее – подразделение ИБ) с ежедневным контролем реализации мер по противодействию компьютерным атакам.

Срок: 30.06.2022.

3. В случае отсутствия подразделения ИБ в Компании принять меры по созданию такого подразделения, обеспечивающего информационную безопасность Компании, а также обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты в Компании, либо с учетом необходимого кадрового и материально-технического усиления, возложить такие функции на существующее структурное подразделение в Компании и/или заключить соответствующий договор со специализированной компанией Группы (инсорсинг).

Срок: 30.06.2022.

4. При заключении договоров на осуществление мероприятий по обеспечению информационной безопасности и повышению уровня информационной безопасности Компании (далее – Договор) должны привлекаться

исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации (далее – экспертные организации) по согласованию с Департаментом информационной безопасности ПАО «Интер РАО».

5. Принять решение о необходимости привлечения экспертных организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты по согласованию с Департаментом информационной безопасности ПАО «Интер РАО». При этом могут привлекаться исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за исключением случая, предусмотренного подпунктом «б» пункта 5. Указа Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250.

Срок: 30.06.2022.

6. Обеспечивать должностным лицам органов Федеральной службы безопасности беспрепятственный доступ (в том числе удалённый) к принадлежащим (используемым) Компанией информационным ресурсам, доступным из информационно-телекоммуникационной сети «Интернет» в целях осуществления мониторинга, предусмотренного подпунктом «в» пункта 5. Указа Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250, а также обеспечивать исполнение указаний, данных органами Федеральной службы безопасности по результатам такого мониторинга.

Срок: постоянно.

7. Обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенций и направляются на регулярной основе в Компании и/или доводятся до Компаний путем рассылок Департамента информационной безопасности ПАО «Интер РАО».

Срок: постоянно.

8. Осуществить мероприятия по оценке уровня защищённости информационных систем Компании, представить отчётные материалы руководителю Департамента информационной безопасности ПАО «Интер РАО» для формирования доклада в Правительство Российской Федерации.

Срок: 20.06.2022.

9. Согласно Указу Президента Российской Федерации от 30.03.2022 № 166, всем заказчикам, **попадающим под действие Федерального закона от 18.07.2011 № 223-ФЗ** «О закупках товаров, работ, услуг отдельными видами юридических лиц» установить запрет на осуществление закупок иностранного программного обеспечения средств защиты информации, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им **значимых объектах**

критической информационной инфраструктуры, а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

Срок: с даты издания настоящего приказа.

10. Для компаний Группы «Интер РАО», **подпадающих под действие Указа Президента Российской Федерации от 01.05.2022 № 250** «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» установить запрет на использование средств защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств прямо или косвенно подконтрольные им либо аффилированные с ними.

Срок: с 01.01.2025.

11. Приостановить проектные и иные мероприятия, предусматривающие необходимость внедрения и/или обновления программного обеспечения в информационной инфраструктуре Компании, за исключением случаев:

11.1 обновления или внедрения программного обеспечения, состоящего на 100% из кода, разработанного компаниями Группы «Интер РАО»;

11.2 обновления или внедрения программного обеспечения (ПО), находящегося в «Едином реестре российских программ для электронных вычислительных машин и баз данных» и «Едином реестре программ для электронных вычислительных машин и баз данных государств - членов Евразийского экономического союза» и прошедшего непосредственно перед обновлением и/или внедрением контрольные процедуры, в соответствии с ВНД МТ-259-1 «Определение требований информационной безопасности при разработке информационных систем»;

11.3 обновления иностранного ПО, включенного в ВНД ИН-021-9 «Обеспечение работников ИТ-оборудованием и ПО» и/или фактически используемого в дочерних обществах в соответствии с ВНД ПТ-016-2 «Техническая политика в области ИТ в Группе «Интер РАО», исключительно при условии успешного прохождения контрольных процедур в соответствии с ВНД МТ-259-1 «Определение требований информационной безопасности при разработке информационных систем» и рекомендаций регуляторов: ФСТЭК России, ФСБ России, Минцифры России и др.;

11.4 обновления или внедрения программного обеспечения АСУ ТП, согласованного к установке Блоком производственной деятельности ПАО «Интер РАО» и экспертной организацией, выбранной по согласованию с Департаментом информационной безопасности ПАО «Интер РАО»;

11.5 проектов и мероприятий, направленных на повышение информационной безопасности информационной инфраструктуры, согласованных Департаментом информационной безопасности ПАО «Интер РАО».

Срок: с даты издания настоящего приказа.

12. Ускорить реализацию проектов и мероприятий, предусмотренных Программой развития информационной безопасности, утвержденной протоколом

решения Правления ПАО «Интер РАО» от 17.12.2020 № 906 в части создания систем безопасности критической информационной инфраструктуры, а также развития центра противодействия кибератакам Группы «Интер РАО», с учетом пп. 9,10.

Срок: 01.05.2023.

13. Реализовать дополнительные организационно-технические мероприятия, связанные с:

13.1 внедрением системы двухфакторной аутентификации при доступе к информационной инфраструктуре Группы «Интер РАО» (за исключением информационных систем, к основным характеристикам которых относится неограниченность доступа, таких как Личные кабинеты клиентов, внешние информационные порталы и сайты-визитки и пр. – далее общедоступные ИС);

Срок: 01.10.2022;

13.2 внедрением системы двухфакторной аутентификации при доступе к общедоступным ИС;

Срок: 31.05.2023;

13.3 организацией дистанционного доступа к информационной инфраструктуре Группы «Интер РАО» (в т.ч. для работников подрядных организаций) с использованием сертифицированных ФСБ России средств криптографической защиты информации в соответствии с Методикой МТ-273-1 «Организация дистанционного пользовательского доступа к информационным ресурсам ПАО «Интер РАО»;

Срок: 31.12.2022;

13.4 организацией доступа к корпоративным информационным системам, доступным в настоящее время из сети Интернет (в т.ч. АСУД, электронная почта и т.п.) за исключением общедоступных ИС, с некорпоративных пользовательских устройств исключительно с использованием сертифицированных ФСБ России средств криптографической защиты информации;

Срок: 31.12.2022;

13.5 ограничением использования сети Интернет в качестве единственного и/или основного канала осуществления взаимодействия информационных и/или автоматизированных систем, обеспечивающих автоматизацию критических процессов Компании, в т.ч. при осуществлении взаимодействия с информационными и/или автоматизированными системами организаций, не входящих в Группу «Интер РАО»;

Срок: 31.12.2022;

13.6 внедрением криптографической защиты каналов связи корпоративной сети передачи данных (далее – КСПД) Компаний Группы «Интер РАО» с применением сертифицированных ФСБ России средств криптографической защиты информации, согласно рекомендациям, определённым п. 10.2 протокола № 906 заседания Правления ПАО «Интер РАО» от 17.12.2022;

Срок: 31.12.2022;

13.7 внедрением криптографической защиты каналов связи локальных вычислительных сетей ЛВС Компаний Группы «Интер РАО» с применением сертифицированных ФСБ России средств криптографической защиты информации;

Срок: 31.05.2023;

13.8 внедрением криптографической защиты каналов связи технологических ЛВС (сетей связи, используемых для взаимодействия автоматизированных систем управления) Компаний Группы при их выходе за пределы установленных в Компаниях Группы контролируемых зон с применением сертифицированных ФСБ России средств криптографической защиты информации;

Срок: 31.12.2022;

13.9 Для компаний Группы «Интер РАО», **подпадающих под действие Указа Президента Российской Федерации от 01.05.2022 № 250** «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», **полным** замещением существующих импортных технических средств защиты информации отечественными аналогами.

Срок: 31.12.2024.

13.10 Для компаний Группы «Интер РАО», **не подпадающих под действие Указа Президента Российской Федерации от 01.05.2022 № 250** «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», **преимущественным** замещением существующих импортных технических средств защиты информации отечественными аналогами, при этом допускается применение существующих средств защиты информации иностранного производства в случае их использования в составе эшелонированной системы информационной безопасности с обязательным дублированием основных функций безопасности средством защиты отечественного производства.

Срок: 31.12.2023.

14. В целях анализа уровня обеспечения информационной безопасности Компаний направлять способом и по форме, определенной Департаментом информационной безопасности ПАО «Интер РАО» и/или Блоком информационных технологий ПАО «Интер РАО» не позднее 1-ой и 3-ей среды каждого календарного месяца в Департамент информационной безопасности ПАО «Интер РАО» и Блок информационных технологий ПАО «Интер РАО» отчет о ходе реализации пункта 1-13 настоящих Рекомендаций.

Приложение № 2 к приказу
ПАО «Интер РАО»
от 09.06.2022 № ИРАО/232

Список компаний Группы «Интер РАО»

№	Наименование компании
1.	АО «Алтайэнергосбыт»
2.	АО «Мосэнергосбыт»
3.	ПАО «Саратовэнерго»
4.	АО «Петербургская сбытовая компания»
5.	ПАО «Тамбовская энергосбытовая компания»
6.	ООО «Орловский энергосбыт»
7.	ООО «Интер РАО –Управление электрогенерацией»
8.	АО «ЕИРЦ Петроэлектросбыт»
9.	ООО «БГК»
10.	ООО «РН-Энерго»
11.	ООО «БашРТС»
12.	ООО «Интер РАО – Цифровые решения»
13.	АО «ТГК-11»
14.	ООО «ОЭК»
15.	АО «Омск РТС»
16.	АО «ТомскРТС»
17.	АО «Томскэнергосбыт»
18.	АО «Томская генерация»
19.	ООО «ЭСКБ»
20.	ООО «ЭСВ»
21.	ООО «ССК»
22.	ООО «Башэнерготранс»
23.	ООО «Интер РАО – Инжиниринг»
24.	АО «ПЭС»
25.	ООО «МосОблЕИРЦ»
26.	АО «ЕИРЦ ЛО»
27.	ООО «ЕИРЦ ТО»
28.	ООО «ЕИРЦ РБ»
29.	ООО «ОРЦ»
30.	ООО «Интер РАО – ИТ»
31.	ООО «Интер РАО - Центр управления закупками»
32.	ООО «Угольный разрез»
33.	АО «Электролуч»
34.	ООО «ИНТЕР РАО – Экспорт»

№	Наименование компании
35.	ООО «Интер РАО – Управление сервисами»
36.	АО «Север»
37.	АО «Интер РАО Капитал»
38.	ООО «ИНТЕР РАО Инвест»