МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

10.03.2022 № 186

Москва

Об утверждении методических рекомендаций по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ

В целях реализации мер по защите объектов информационной инфраструктуры Российской Федерации, предусматривающих обеспечение целостности и доступности информации,

ПРИКАЗЫВАЮ:

утвердить прилагаемые Методические рекомендации по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ.

Министр М.И. Шадаев

УТВЕРЖДЕНЫ
приказом Министерства цифрового
развития, связи и массовых
коммуникаций Российской Федерации
от «10» 03 2022 г. № 186

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ

Настоящие Методические рекомендации по обеспечению информационной безопасности государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ (далее – Методические рекомендации) определяют перечень организационных мероприятий, которые рекомендуется реализовать государственным корпорациям, компаниям с государственным участием, а также их дочерним организациям и зависимым обществам (далее – государственные корпорации, государственные компании) в целях противодействия компьютерным атакам и другим угрозам в сфере информационной безопасности.

В целях обеспечения необходимого уровня информационной безопасности государственным корпорациям, государственным компаниям, их дочерним и зависимым обществам рекомендуется:

1. Обеспечить на постоянной основе реализацию организационно-технических мер, предусмотренных нормативными правовыми актами, а также методическими рекомендациями, письмами и иными документами ФСБ России и ФСТЭК России (далее – организационно-технические меры).

До 18 марта 2022 г.:

2. Возложить на лиц из числа заместителей руководителя полномочия по обеспечению информационной безопасности, а также обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в организации (далее – ответственный по информационной безопасности). Ответственному по информационной безопасности проработать необходимость кадрового и материально-технического усиления подразделения организации по информационной безопасности и обеспечивать постоянный контроль за реализацией мер по противодействию компьютерным атакам и другим угрозам в сфере информационной безопасности.

3. Принять решение о необходимости заключения договоров на оказание услуг по повышению уровня информационной безопасности организации с экспертными организациями в сфере обеспечения информационной безопасности, под которыми понимаются юридические лица или индивидуальные предприниматели, оказывающие услуги по противодействию компьютерным атакам и компьютерным

инцидентам, имеющие соглашение с ФСБ России или Национальным координационным центром по компьютерным инцидентам о взаимодействии в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, в целях обеспечения информационной безопасности (далее – экспертные организации).

4. Организовать взаимодействие с операторами связи, а также экспертными организациям для обеспечения защиты государственной организации, государственной компании от распределенных компьютерных атак типа «отказ в обслуживании» на сетевом и прикладном уровнях (L3, L7).

До 11 апреля 2022 г.:

5. Провести мероприятия, предусмотренные указанными договорами на оказание услуг по повышению уровня информационной безопасности организации с экспертными организациями в сфере обеспечения информационной безопасности.

6. Организовать еженедельное направление не позднее предпоследнего рабочего дня календарной недели в Минцифры России, ФСБ России и ФСТЭК России в целях анализа уровня обеспечения информационной безопасности государственных корпораций, государственных компаний, их дочерних и зависимых обществ отчета о реализации настоящих Методических рекомендаций, а также обеспечить участие ответственных по информационной безопасности в соответствующих совещаниях, проводимых Минцифры России.