Инструкция по выполнению требований законодательства Российской Федерации о защите критической информационной инфраструктуры организациями, осуществляющими деятельность в сфере оборонной, металлургической и химической промышленности

1. Организациям, подведомственным или находящимся в сфере ведения Минпромторга России, не завершившим работу по определению наличия объектов критической информационной инфраструктуры и их категорированию:

1.1. Создать постоянно действующую комиссию по категорированию в соответствии с требованиями пункта 11 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127[1] (далее – Правила категорирования объектов критической информационной инфраструктуры).

1.2. Провести инвентаризацию всех информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, которые на праве собственности, аренды или на ином законном основании принадлежат организации.

1.3. Провести работу по определению наличия объектов критической информационной инфраструктуры с учётом всех имеющихся в организации информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, в том числе таких как:

локальные вычислительные сети;

информационные системы, предназначенные для разработки и хранения конструкторской документации;

испытательные стенды;

лабораторное оборудование;

системы цифрового моделирования;

информационные системы управления хозяйственной деятельностью, реализующие функции стратегического планирования (BPM-системы, OLAP-системы);

информационные системы управления ресурсами, позволяющие осуществлять планирование, учет, контроль и анализ ресурсов (EPR-системы);

информационные системы, обеспечивающие управлением жизненным циклом продукции (PLM-системы);

информационные системы управления производственными ресурсами в ходе технологического процесса (MES-системы);

[1] С изменениями, утверждёнными постановлениями Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127», от 24 декабря 2021 г. № 2431«О внесении изменений в постановление Правительства Российской Федерации»

автоматизированные системы, обеспечивающие контроль и (или) управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (SCADA-системы, распределенные системы управления);

информационные (автоматизированные) системы управления станками с числовым программным управлением.

1.4. При наличии в организации указанных систем сформировать перечень объектов критической информационной инфраструктуры, подлежащих категорированию, и в соответствии с пунктом 15 Правил категорирования объектов критической информационной инфраструктуры согласовать с:

Заместителем Министра промышленности и торговли Российской Федерации В.В. Шпаком (только подведомственным Минпромторгу России организациям);

головными организациями интегрированных структур (организациям, входящим в состав интегрированных структур).

1.5. Направить в ФСТЭК России согласованный и утвержденный перечень объектов критической информационной инфраструктуры, подлежащих категорированию, в соответствии с пунктом 15 Правил категорирования объектов критической информационной инфраструктуры в печатном и электронном виде.

Срок направления: в течение 5 рабочих дней после утверждения перечня.

1.6. Направить в ФСТЭК России сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий, в соответствии с пунктом 5 статьи 7 Федерального закона № 187-ФЗ и пунктом 18 Правил категорирования объектов критической информационной инфраструктуры в печатном и электронном виде по форме, утверждённой приказом ФСТЭК России от 22 декабря 2017 г. № 236, в порядке, установленном информационным сообщением ФСТЭК России от 17 апреля 2020 г. № 240/84/611.

1.7. Направить результаты выполнения решений, изложенных в пунктах № 1.1 – 1.5, по форме № 1 (образец формы прилагается) в печатном и электронном виде на оптическом диске в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

1.8. Для вновь создаваемых и проектируемых информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления выполнять требования пунктов 8, 18 Правил категорирования объектов критической информационной инфраструктуры.

При этом сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий направляются в ФСТЭК России в печатном и электронном виде по форме, утверждённой приказом ФСТЭК России от 22 декабря 2017 г. № 236 в порядке, установленном информационным сообщением ФСТЭК России от 17 апреля 2020 г. N 240/84/611.

2. Организациям, подведомственным или находящимся в сфере ведения Минпромторга России, выполнившим работу по категорированию объектов критической информационной инфраструктуры и имеющим значимые объекты критической информационной инфраструктуры:

2.1. Создать систему значимых объектов безопасности критической информационной инфраструктуры в соответствии с «Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. № 50118), при этом:

возложить на руководителя субъекта критической информационной инфраструктуры или уполномоченное им лицо функции по созданию системы безопасности, организации и контролю ее функционирования;

создать или определить структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – структурное подразделение по безопасности), или назначить отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – специалисты по безопасности);

структурному подразделению по безопасности, специалистам по безопасности реализацию функций проводить во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры, иными подразделениями (работниками), участвующими в обеспечении безопасности значимых объектов критической информационной инфраструктуры;

применять для обеспечения безопасности значимых объектов критической информационной инфраструктуры сертифицированные на соответствие требованиям безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;

разработать и утвердить организационно-распорядительные документы по безопасности значимых объектов критической информационной инфраструктуры, определяющие порядок и правила функционирования системы безопасности значимых объектов критической информационной инфраструктуры,

а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры;

разработать план мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры на год;

организовать и проводить ежегодный внутренний контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер.

2.2. Организовать в 2022 году и последующие годы профессиональную переподготовку, повышение квалификации работников структурных подразделений по безопасности или специалистов по безопасности по профессиональным программам в области обеспечения безопасности объектов критической информационной инфраструктуры, согласованным ФСТЭК России.

2.3. Для обеспечения устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак руководствоваться «Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239 (зарегистрировано Минюстом России 26 марта 2018 г. № 50524).

2.4. В случае изменения сведений, указанных в подпунктах «а» – «е» пункта 17 Правил категорирования объектов критической информационной инфраструктуры,[2] направлять в ФСТЭК России новые сведения в печатном и электронном виде по форме, предусмотренной пунктом 18 Правил категорирования объектов критической информационной инфраструктуры.

Срок направления: не позднее 20 рабочих дней со дня изменения сведений.

2.5. Направить сведения о результатах реализации положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изданных в его исполнение нормативных правовых актов по форме № 1 (образец формы прилагается) в печатном и электронном виде на оптическом диске в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

2.6. Подготовить и направить «Паспорт системы обеспечения безопасности значимых объектов критической информационной инфраструктуры в организации» в печатном и электронном виде (образец формы паспорта прилагается) в:

[2] С учетом внесенных изменений, утверждённых постановлением Правительства Российской Федерации от 24 декабря 2021 г. № 2431«О внесении изменений в постановление Правительства Российской Федерации»

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

Сроки направления: к 1 июля 2023 г., далее ежегодно к 1 сентября (с учетом внесенных изменений).

2.7. Разработать и согласовать «План мероприятий, реализуемых организацией при установлении в отношении принадлежащих ей объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак»[3] с ФСТЭК России.

2.8. Направить в ФСТЭК России и управления ФСТЭК России по федеральным округам копию утвержденного «Плана мероприятий, реализуемых организацией при установлении в отношении принадлежащих ей объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак».[4]

2.9. Направлять информацию о выполнении пунктов 2.7 и 2.8 в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

[3] Разрабатывается в соответствии с «Порядком установления уровня опасности проведения целевых компьютерных атак на информационную инфраструктуру Российской Федерации», утвержденным распоряжением Секретаря Совета Безопасности Российской Федерации от 14 декабря 2020 г. № А21-68рсб

[4] В соответствии с пунктом 14 «Методического документа «Рекомендации по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры Российской Федерации при установлении в отношении принадлежащим им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак», утвержденного ФСТЭК России 9 августа 2021 г.