Приказ ФСБ России от 24.07.2018 № 366 "О Национальном координационном центре по компьютерным инцидентам"

В соответствии с частью 4 статьи 5 и пунктом 2 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"<1>, приказываю:

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

1. Создать Национальный координационный центр по компьютерным инцидентам.
2. Утвердить прилагаемое Положение о Национальном координационном центре по компьютерным инцидентам.

Директор

А. БОРТНИКОВ

Приложение

к приказу ФСБ РФ

от 24 июля 2018 г. N 366

ПОЛОЖЕНИЕ О НАЦИОНАЛЬНОМ КООРДИНАЦИОННОМ ЦЕНТРЕ ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

1. Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты"<1>.

2. НКЦКИ в своей деятельности руководствуется законодательством Российской Федерации, ведомственными (межведомственными) нормативными правовыми актами, в том числе настоящим Положением, а также международными договорами Российской Федерации.

3. Задачей НКЦКИ является обеспечение координации деятельности субъектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных

атак и реагирования на компьютерные инциденты.

4. В целях выполнения предусмотренной настоящим Положением задачи НКЦКИ осуществляет следующие функции:

4.1. Координирует мероприятия по реагированию на компьютерные инциденты и непосредственно участвует в таких мероприятиях.

4.2. Организует и осуществляет обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в том числе посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными (далее - техническая инфраструктура НКЦКИ).

4.3. Осуществляет методическое обеспечение деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

4.4. Участвует в обнаружении, предупреждении и ликвидации последствий компьютерных атак.

4.5. Обеспечивает своевременное доведение до субъектов критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

4.6. Осуществляет сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

4.7. Осуществляет эксплуатацию, обеспечение функционирования и развитие технической инфраструктуры НКЦКИ.

4.8. Организует получение информации, представляемой в соответствии с законодательством Российской Федерации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, а также информации, которая может представляться иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и

международными.

4.9. Определяет необходимые для организации взаимодействия форматы представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и доводит их до субъектов критической информационной инфраструктуры.

4.10. Определяет состав технических параметров компьютерного инцидента, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и доводит его до субъектов критической информационной инфраструктуры.

5. В целях выполнения предусмотренных настоящим Положением задачи и функций НКЦКИ в пределах своей компетенции имеет право:

5.1. Направлять уведомления и запросы субъектам критической информационной инфраструктуры, а также иным не являющимся субъектами критической информационной инфраструктуры органам и организациям, в том числе иностранным и международным, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

5.2. Отказывать в предоставлении информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, по запросам органа иностранного государства или международной организации, не обладающих полномочиями направлять такой запрос, а также в случаях, когда предоставление такой информации создает угрозу безопасности Российской Федерации.

5.3. Создавать рабочие группы из представителей субъектов критической информационной инфраструктуры по согласованию с их руководством для решения вопросов, отнесенных к компетенции НКЦКИ.

5.4. Привлекать к реагированию на компьютерные инциденты организации и экспертов, осуществляющих деятельность в данной области.

5.5. Распространять и публиковать информационные и справочные материалы, участвовать в работе научно-технических конференций, симпозиумов, совещаний, выставок, в том числе международных, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

5.6. Заключать от своего имени соглашения о сотрудничестве в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

6. Информационно-аналитическое, организационное и материально-техническое обеспечение НКЦКИ

осуществляется Центром защиты информации и специальной связи ФСБ России.

7. НКЦКИ возглавляет директор НКЦКИ, которым является заместитель руководителя Научно-технической службы - начальник Центра защиты информации и специальной связи ФСБ России.

8. Директор НКЦКИ:

8.1. Организует деятельность НКЦКИ.

8.2. Осуществляет от имени НКЦКИ взаимодействие с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

8.3. Утверждает положения о рабочих группах НКЦКИ, создаваемых в соответствии с пунктом 5.3 настоящего Положения, и персональный состав таких рабочих групп.

9. НКЦКИ имеет бланк со своим наименованием и эмблему.

<1> Пункт 2 части 2 статьи 5 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".