

## Регламент взаимодействия

**Национального координационного центра по компьютерным инцидентам с Регистратором по противодействию использованию доменных имен (в доменах .PP.RU, .NET.RU, .ORG.RU) в целях: осуществления фишинга, несанкционированного доступа в информационные системы третьих лиц (пользователей, посетителей), распространения вредоносных программ, управления вредоносными программами (управление бот-сетью)**

В целях взаимодействия Национального координационного центра по компьютерным инцидентам (в дальнейшем – Организация) с Регистратором по противодействию использованию доменных имен (в доменах .PP.RU, .NET.RU, .ORG.RU) в целях: осуществления фишинга, несанкционированного доступа в информационные системы третьих лиц (пользователей, посетителей), распространения вредоносных программ, управления вредоносными программами (управление бот-сетью), устанавливаются следующие положения:

**1.** Организация создаёт информационный ресурс, позволяющий собирать информацию от участников информационных процессов (в том числе иностранных) об использовании доменных имен (в доменах .PP.RU, .NET.RU, .ORG.RU) в целях: осуществления фишинга, несанкционированного доступа в информационные системы третьих лиц (пользователей, посетителей), распространения вредоносных программ, управления вредоносными программами (управление бот-сетью).

**1.1.** Организация создаёт уникальный электронный почтовый адрес, являющийся в дальнейшем аутентификационным признаком принадлежности передаваемой информации. Данным адресом является: [incident@cert.gov.ru](mailto:incident@cert.gov.ru).

**1.2.** Сбор информации от участников информационных процессов осуществляется:

- по телефонному номеру в круглосуточном режиме: +7 (916) 901-07-42;
- по адресу электронной почты [incident@cert.gov.ru](mailto:incident@cert.gov.ru) (круглосуточно);
- через сайт <http://cert.gov.ru/>

**2.** Организация обрабатывает поступившую информацию об использовании доменных имен (в доменах .PP.RU, .NET.RU, .ORG.RU) в целях: осуществления фишинга, несанкционированного доступа в информационные системы третьих лиц (пользователей, посетителей), распространения вредоносных программ, управления вредоносными программами (управление бот-сетью), уведомляет Регистратора о выявленных нарушениях и в случае необходимости, запрашивает дополнительную информацию у Регистратора.

**3.** Организация направляет обработанную информацию Регистратору доменного имени для принятия мер, предусмотренных данным Регламентом.

**3.1.** В своем сообщении Регистратору Организация обязана указать:

- полное наименование/название доменного имени: доменное имя .TLD, где TLD – домен верхнего уровня/зона (Top-level domain);
- полученные сведения о факте использования доменного имени в целях указанных в пункте 1 настоящего Регламента.

**4.** Сообщения от Организации должны направляться Регистратору только в кодировке win-1251 либо koï8-R, в формате, определенным RFC-822, с электронного почтового адреса: incident@cert.gov.ru.

**5.** Регистратор, получив электронное сообщение от Организации, незамедлительно подтверждает получение информации:

- на каждое полученное сообщение автоматически генерируется и высылается на адрес отправителя письмо-подтверждение о получении сообщения с указанием присвоенного данному сообщению уникального номера/идентификатор [название регистратора.ru#: ].

**6.** При получении сообщения от Организации Регистратор принимает решение:

- о приостановке делегирования соответствующего доменного имени в доменах .PP.RU, .NET.RU, .ORG.RU, Организация информирует о принятом Регистратором решении Координатора и лицо, представившее информацию о нарушении, и осуществляет последующий мониторинг возможности доступа к соответствующему доменному имени.
- не приостанавливать делегирование доменного имени доменах .PP.RU, .NET.RU, .ORG.RU, Организация информирует об этом Координатора и лицо, представившее информацию о нарушении, и оставляет за собой право согласиться с принятым решением, или же осуществить дополнительную проверку информации о нарушении, провести анализ данных и материалов, запросить дополнительные сведения и вновь направить сообщение Регистратору.

**7.** Настоящий Регламент прекращает свое действие в случае утраты Организацией статуса Компетентной организации, на основании пункта 5.7.7 Правил регистрации доменных имен в доменах .PP.RU, .NET.RU, .ORG.RU от 1 января 2015 года.