

Регламент взаимодействия

АНО «Центр реагирования на компьютерные инциденты» 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 АНО «Центр реагирования на компьютерные инциденты» 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. Компания 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. Компания создаёт уникальный электронный почтовый адрес, являющийся в дальнейшем аутентификационным признаком принадлежности передаваемой информации. Данным адресом является: adverse@cert.ru.

1.2. Сбор информации от участников информационных процессов осуществляется:

- по адресу электронной почты adverse@cert.ru;
- через web-форму на сайте <http://www.cert.ru/ru/abuse.shtml>.

2. Компания 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. Компания направляет обработанную информацию Регистратору доменного имени для принятия мер, предусмотренных данным Регламентом.

3.1. В своем сообщении Регистратору Компания 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.

3.2. Сообщения от Компании должны направляться Регистратору строго в кодировке win1251 либо koi8-R, в формате, определенным RFC-822 с электронного почтового адреса: adverse@cert.ru.

4. Регистратор, получив электронное сообщение от Компании, 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#:].

5. При получении сообщения от Компании Регистратор принимает решение:

- о приостановке делегирования соответствующего доменного имени в доменах .PP.RU, .NET.RU, .ORG.RU, Компания 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, Компания 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.

6. Настоящий Регламент прекращает свое действие в случае утраты Компанией статуса Компетентной организации, на основании п. 5.7. 7 (Правил регистрации доменных имен в доменах .PP.RU, .NET.RU, .ORG.RU от 01.01.2015 года).