УТВЕРЖДАЮ
Директор Национального
координационного центра по
компьютерным инцидентам

О.В. Скрябин
«02» 09 2024 г.

РЕГЛАМЕНТ

взаимодействия Национального координационного центра по компьютерным инцидентам и владельцев информационных ресурсов Российской Федерации при информировании Федеральной службы безопасности Российской Федерации о компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак

№149/2/6-1000

1. Общие положения

1.1 Настоящий регламент определяет порядок взаимодействия владельцев информационных ресурсов Российской Федерации (далее – субъект ГосСОПКА) с Национальным координационным центром по компьютерным инцидентам при информировании Федеральной службы безопасности Российской Федерации о компьютерных инцидентах и компьютерных атаках на информационных ресурсах, находящихся в их зоне ответственности.

2. Термины и определения

2.1 Значимый объект критической информационной инфраструктуры (ЗОКИИ) – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

2.2 Зона ответственности субъекта ГосСОПКА – информационные ресурсы, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирования на компьютерные инциденты.

2.3 Информационные ресурсы (ИР) – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления.

2.4 Компьютерная атака (КА) – целенаправленное воздействие программных и (или) программно-аппаратных средств на ИР, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими ИР информации.

2.5 Компьютерный инцидент (КИ) – факт нарушения и (или) прекращения функционирования ИР, сети электросвязи, используемой для организации взаимодействия таких ИР, и (или) нарушения безопасности обрабатываемой таким ИР информации, в том числе произошедший в результате компьютерной атаки.

2.6 Конфиденциальная информация – информация, в отношении которой ее обладателем введен режим конфиденциальности и бумажный или электронный носитель такой информации содержит реквизиты, позволяющие однозначно ее отнести к конфиденциальной информации.

2.7 Критическая информационная инфраструктура (КИИ) – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

2.8 Национальный координационный центр по компьютерным инцидентам (НКЦКИ) – организация, осуществляющая на национальном уровне координацию деятельности владельцев ИР по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

2.9 Объекты КИИ (ОКИИ) – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ.

3. Функции участников информационного взаимодействия

3.1 При решении задач по обмену информацией о КИ, связанных с функционированием ИР, осуществляются следующие функции.

3.1.1 НКЦКИ:

– доводит до субъекта ГосСОПКА информацию об угрозах безопасности информации и о необходимых мерах по противодействию им;

– доводит до субъекта ГосСОПКА информацию о средствах и способах проведения КА и о методах их обнаружения, предупреждения и противодействия им;

– доводит до субъекта ГосСОПКА информацию о признаках КИ, связанных с функционированием ИР субъекта ГосСОПКА;

– оказывает содействие в реагировании на КИ, связанные с функционированием ИР, при наличии такой необходимости, обеспечивает методическую и экспертную поддержку по вопросам реагирования на КИ;

– определяет состав и форматы предоставляемой субъектом ГосСОПКА информации о КИ, связанных с функционированием ИР.

3.1.2 Субъект ГосСОПКА:

– предоставляет в НКЦКИ первичные инвентаризационные сведения[1];

– своевременно актуализирует сведения об ИР, находящихся в зоне ответственности субъекта ГосСОПКА;

– предоставляет в НКЦКИ сведения о выявляемых КИ, связанных с функционированием ИР, и КА на ИР, находящихся в зоне ответственности субъекта ГосСОПКА, а также информацию о предпринятых мерах, результатах реагирования на такие инциденты и ликвидации последствий КА[2];

– принимает от НКЦКИ и реализует информацию об актуальных угрозах безопасности и необходимых мерах по противодействию им, о средствах и способах проведения КА и методах их обнаружения, предупреждения и противодействия им, а также о признаках КИ, связанных с функционированием ИР.

4. Перечень передаваемой информации

4.1 В рамках взаимодействия между НКЦКИ и субъектами ГосСОПКА передается информация:

– о КИ и КА в соответствии с утвержденными НКЦКИ форматами, в том числе требующих содействия в реагировании со стороны НКЦКИ;

– о признаках КИ, связанных с функционированием ИР, в соответствии с форматами, утвержденными НКЦКИ;

– о мерах, предпринятых для локализации КИ, связанных с функционированием ИР, а также о результатах этих мер;

– о выявленных угрозах безопасности информации, реализация которых может повлиять на штатное функционирование ИР и о необходимых мерах по противодействию им;

---

[1] Информация передается в формате excel в электронном виде или через Личный кабинет

[2] Передается строго в соответствии с форматами, разработанными НКЦКИ

– о средствах и способах проведения КА и о методах их обнаружения, предупреждения и противодействия им;

– запросы на получение дополнительных сведений об угрозах безопасности информации и вредоносной активности;

– сведения об ИР в зоне ответственности субъекта ГосСОПКА.

5. Каналы взаимодействия

5.1 При передаче информации, указанной в разделе 4 Регламента, в качестве основных каналов передачи информации в адрес НКЦКИ используются:

5.1.1 Средства автоматизированного обмена информацией на основе программного интерфейса (посредством API).

5.1.2 Личный кабинет субъекта ГосСОПКА, функционирующий в технической инфраструктуре НКЦКИ (далее – ТИ НКЦКИ).

5.1.3 Электронная почта.

5.2 В качестве дополнительных каналов передачи информации используются:

5.2.1. Почтовые отправления (с приложением электронных носителей информации).

5.2.2. Телефонная связь.

6. Порядок взаимодействия участников информационного обмена

6.1 Информации о КИ, связанных с функционированием ИР, находящихся в зоне ответственности субъекта ГосСОПКА, передаваемой в НКЦКИ посредством каналов, указанных в подпунктах 5.1.1-5.1.2 Регламента, в ТИ НКЦКИ присваивается уникальный идентификатор КИ (ID).

6.2 Информация о КИ, связанных с функционированием ИР, передаваемая посредством каналов, указанных в подпунктах 5.1.3, 5.2.1 и 5.2.2 Регламента, учитывается сотрудниками НКЦКИ в ТИ НКЦКИ, после чего в адрес отправителя информации передается ID по тем же каналам.

6.3 При передаче дополнительной информации о КИ, связанных с функционированием ИР, в НКЦКИ вне зависимости от канала передачи информации необходимо использовать присвоенный ранее ID.

6.4 При направлении в адрес субъекта ГосСОПКА информации о признаках КИ, связанных с функционированием ИР, данному уведомлению присваивается идентификатор.

7. Сроки предоставления информации

7.1 Информация о КИ, связанном с функционированием ЗОКИИ, в соответствии с пунктом 4 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденного приказом ФСБ России от 19 июня 2019 г. № 282, направляется субъектом ГосСОПКА в НКЦКИ в срок не позднее 3 часов с момента обнаружения КИ.

7.2 Информация о КИ, связанном с функционированием иных ИР, находящихся в зоне ответственности субъекта ГосСОПКА – в срок не позднее 24 часов с момента его обнаружения.

7.3 Сведения об изменении внешних сетевых реквизитов ИР, находящихся в зоне ответственности субъекта ГосСОПКА, направляются им в адрес НКЦКИ в срок не более 2-х рабочих дней с момента получения информации данной категории субъектом ГосСОПКА.

7.4 Сведения об изменении контактных данных направляются в адрес НКЦКИ в срок не более 5-ти дней с момента назначения нового лица/подразделения ответственным за взаимодействие с НКЦКИ.

7.5 При получении от субъекта ГосСОПКА сведений о КИ и КА НКЦКИ в течение 24 часов направляет ответ о результатах их рассмотрения.

7.6 Сведения, перечисленные в первом, втором и третьем дефисах подпункта 3.1.1, НКЦКИ направляет по выбранному субъектом ГосСОПКА каналу в течение 24 часов с момента получения таких сведений.

8. Обмен конфиденциальной информацией

8.1 Информационные сообщения и запросы, передаваемые по каналам взаимодействия, предусмотренным подпунктами 5.1.1-5.1.3, 5.2.2 Регламента, не должны содержать информацию, составляющую государственную тайну.

8.2 Стороны обязуются сохранять конфиденциальную информацию в течение 5 лет и принимать все необходимые меры для ее защиты, в том числе в случае реорганизации или ликвидации Сторон, а также в случае прекращения действия (расторжения) Регламента.

8.3 Стороны настоящим обязуются не разглашать и не допускать разглашения конфиденциальной информации третьим лицам без предварительного письменного согласия другой стороны.

8.4 Передача конфиденциальной информации третьим лицам в целях реализации функций НКЦКИ осуществляется при условии ее обязательного обезличивания. При этом под обезличиванием понимается отсутствие в передаваемых данных сведений, позволяющих однозначно идентифицировать ИР, находящиеся в зоне ответственности субъекта ГосСОПКА, вовлеченные в КИ.

8.5 Стороны рассматривают настоящий раздел Регламента как соглашение (договор) о конфиденциальности.

9. Контактные данные

9.1 Контактные данные НКЦКИ:

- сетевой адрес портала НКЦКИ в сети Интернет: cert.gov.ru;
- адрес Личного кабинета субъекта ГосСОПКА: https://lk.cert.gov.ru;
- адрес электронной почты для обмена информацией, касательно компьютерных инцидентов: incident@cert.gov.ru;

– адрес электронной почты для взаимодействия по остальным вопросам: info@cert.gov.ru;

– адрес электронной почты для рассылки бюллетеней об угрозах безопасности информации и о необходимых мерах по противодействию им: threats@cert.gov.ru;

– адрес электронной почты для организации подключения к ТИ НКЦКИ: network@cert.gov.ru;

– почтовый адрес: 107031, г. Москва, ул. Большая Лубянка, д. 1/3;

– контактный телефон по вопросам КИ и КА: +7(980)162-28-40;

– контактный телефон по иным вопросам: +7 (916) 901-07-42.

10. Сроки, порядок заключения и расторжения Регламента

10.1 Для заключения Регламента субъект ГосСОПКА официальным письмом:

– информирует НКЦКИ о намерении взаимодействия с НКЦКИ и выражает согласие с положениями данного Регламента;

– предоставляет контактные данные специалистов, ответственных за взаимодействие с НКЦКИ;

– предоставляет первичную инвентаризационную информацию в электронном виде.

10.2 Датой вступления в силу Регламента является дата подписания письма от НКЦКИ в адрес субъекта ГосСОПКА о заключении Регламента. Письмо НКЦКИ об установлении взаимодействия будет направлено в адрес субъекта ГосСОПКА почтой с направлением копии на адрес электронной почты, указанный субъектом ГосСОПКА.

10.3 Настоящий Регламент может быть расторгнут по согласованию Сторон, а также по инициативе одной из Сторон посредством письменного уведомления об этом другой Стороны не позднее чем за 30 дней до дня прекращения его действия.

10.4 Изменения и дополнения вносятся в Регламент путем утверждения НКЦКИ новой редакции Регламента, о чем не позднее следующего за утверждением

дня извещается субъект ГосСОПКА. Новый Регламент заключается в соответствии с порядком, установленном в настоящем пункте.

До получения субъектом ГосСОПКА уведомления от НКЦКИ о заключении нового Регламента действует ранее заключенный Регламент.