УТВЕРЖДАЮ
Директор Национального
координационного центра
по компьютерным
инцидентам

О.В. Скрябин
«02» 09 2024 г.

**Методические рекомендации по организации прямого взаимодействия с Национальным координационным центром по компьютерным инцидентам**

## 1. Общие положения

Настоящий документ предназначен для владельцев российских информационных ресурсов и содержит описание процедуры организации взаимодействия с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ). Методические рекомендации описывают цели организации взаимодействия, перечень передаваемых сведений, а также возможные каналы взаимодействия.

Рекомендации, указанные в настоящем документе, не относятся к владельцам российских информационных ресурсов, организовавших взаимодействие с НКЦКИ через Центр ГосСОПКА.

НКЦКИ осуществляет свою деятельность в соответствии с Положением, утвержденным приказом ФСБ России от 24 июля 2018 № 366 «О Национальном координационном центре по компьютерным инцидентам».

Деятельность НКЦКИ направлена на повышение защищенности российских информационных ресурсов, повышение осведомленности о методах проведения компьютерных атак (далее – КА) и способах противодействия им, помощь организациям в реагировании на компьютерные инциденты, связанные с функционированием информационных ресурсов (далее – КИ, связанные с функционированием ИР).

Задачей НКЦКИ является обеспечение координации деятельности субъектов критической информационной инфраструктуры (далее – КИИ) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

## 2. Участники взаимодействия

К организациям, для которых взаимодействие с НКЦКИ по вопросам реагирования на КИ, связанные с функционированием ИР, и угрозы безопасности информации является обязательным, относятся:

— субъекты КИИ на основании Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

— федеральные органы исполнительной власти, высшие исполнительные органы государственной власти субъектов Российской Федерации, государственные фонды, государственные корпорации (компании) и иные организации, созданные на основании федеральных законов, стратегические предприятия, стратегические акционерные общества и системообразующие организации российской экономики на основании Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

— операторы персональных данных на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

— провайдеры хостинга на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 1 ноября 2023 г. № 936 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет».

Иные организации, не относящиеся к указанным категориям, вправе добровольно осуществлять взаимодействие с НКЦКИ по вопросам обнаружения КА и реагирования на КИ, связанные с функционированием ИР.

Указанные организации являются субъектами ГосСОПКА.

## 3. Цели взаимодействия

НКЦКИ организован и развивается механизм взаимодействия владельцев российских информационных ресурсов, при котором опыт и возможности одних субъектов используются для повышения защищенности всех остальных.

Взаимодействие осуществляется по двум основным направлениям:

1. Содействие в реагировании на КИ, связанные с функционированием ИР, произошедший у субъекта ГосСОПКА. Такое содействие может оказываться НКЦКИ в следующих формах:

– оказание консультативной помощи. Специалистами НКЦКИ могут оперативно предоставляться субъекту ГосСОПКА рекомендации по противодействию вредоносной активности, сведения о которой имеются в НКЦКИ.

– координация мероприятий по реагированию на КИ, связанные с функционированием ИР, с привлечением сторонних организаций (ЦМУ ССОП и операторов связи для фильтрации трафика, хостинг-провайдеров для прекращения работы вредоносных ресурсов, экспертов ведущих отечественных компаний в области информационной безопасности для выработки способов противодействия КА и др.).

– непосредственное участие сотрудников НКЦКИ в реагировании на КИ, связанные с функционированием ИР. Данный вид взаимодействия предполагает подписание отдельного регламента.

2. Сбор и распространение сведений об угрозах безопасности информации, способах и средствах проведения КА для принятия субъектами ГосСОПКА мер по предотвращению КИ, связанных с функционированием ИР. В том случае, если субъект ГосСОПКА успешно справился с компьютерным инцидентом, он направляет в НКЦКИ технические сведения о вредоносной активности, с проявлениями которой он столкнулся.

В НКЦКИ используется формализованное описание категорий компьютерных инцидентов и технических параметров каждого из них.

НКЦКИ осуществляет сбор сведений об источниках вредоносных воздействий, о произошедших КИ, связанных с функционированием ИР, об угрозах проведения атак, о состоянии защищенности, об уязвимостях программного обеспечения и т. д. Эти данные собираются на уровне объектов, обогащаются сведениями от ведущих отечественных компаний и экспертов, международных центров реагирования на компьютерные инциденты, результатами собственных исследований НКЦКИ и используются НКЦКИ для выявления признаков КИ, связанных с функционированием ИР других субъектов, а также организации мероприятий по противодействию данному типу вредоносной активности в масштабах российского информационного пространства.

В целых оперативного и адресного доведения информации до владельцев информационных ресурсов НКЦКИ собирает от субъектов ГосСОПКА следующую инвентаризационную информацию:

– сведения о всех внешних IP-адресах субъекта ГосСОПКА;
– сведения о всех внешних доменных именах субъекта ГосСОПКА;
– сведения о доменном имени почтового сервера.

На основе получаемой и анализируемой информации НКЦКИ предоставляет субъектам ГосСОПКА следующие сведения:

– данные о признаках КИ, связанных с функционированием ИР субъекта ГосСОПКА;
– индикаторы вредоносной активности (IOC) — те сведения, которые могут использоваться для выявления, прежде всего автоматизированными средствами, различных видов вредоносной активности;
– данные об уязвимостях программного обеспечения;
– оперативные сведения о готовящихся компьютерных атаках;
– рекомендации по нейтрализации актуальных угроз безопасности.

## 4. Передаваемые сведения

В рамках взаимодействия НКЦКИ и субъектов ГосСОПКА может передаваться следующая информация:

– о КИ, связанных с функционированием ИР, в том числе требующих содействия в реагировании со стороны НКЦКИ;

– о КА на ИР субъекта ГосСОПКА;

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

– 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;

– 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, находящихся в зоне ответственности субъекта ГосСОПКА.

## 5. Порядок организации взаимодействия

Состав и форматы представления сведений, передаваемых между субъектами ГосСОПКА и НКЦКИ, сроки и порядок их направления, контактные данные сторон и другие вопросы взаимодействия определяются в «Регламенте 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» (далее – Регламент).

Регламент утверждается Директором НКЦКИ и размещается на официальном сайте НКЦКИ в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

В целях упрощения процедуры подписания Регламента НКЦКИ поддерживается ее осуществление в форме присоединения. Для вступления в силу Регламента субъект ГосСОПКА направляет на имя Директора НКЦКИ письмо на бланке организации на бумажном носителе за подписью руководителя организации.

В письме должно быть выражено согласие с положениями Регламента[1], а также указаны контактные данные специалистов, ответственных за взаимодействие[2].

Для обеспечения преемственности при смене ответственных за взаимодействие сотрудников субъекта ГосСОПКА, оперативности обмена информацией и непрерывности взаимодействия рекомендуем в качестве контактных данных указывать электронный адрес и телефон подразделения по обеспечению информационной безопасности и дополнительно контактные

---

[1] Размещен на официальном сайте НКЦКИ в информационно-телекоммуникационной сети «Интернет» по адресу: «www.cert.gov.ru»

[2] Образец письма в НКЦКИ приведен в Приложении 1

данные руководителя подразделения, ответственного за обеспечение информационной безопасности, а также своевременно актуализировать сведения.

В случае выбора варианта взаимодействия через электронную почту необходимо определить единый адрес для взаимодействия с НКЦКИ. Информирование об инцидентах и атаках должно осуществляться с указанного адреса. НКЦКИ также будет направлять сообщения на этот адрес электронной почты.

К письму необходимо приложить на электронном носителе инвентаризационную информацию или направить ее на электронную почту info@cert.gov.ru.

Первичная инвентаризационная информация заполняется в виде трех таблиц формата «.excel». Шаблоны таблиц размещены и доступны для скачивания на официальном сайте НКЦКИ в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

Ответное письмо НКЦКИ об установлении взаимодействия будет направлено в адрес субъекта ГосСОПКА почтой с направлением копии на адрес электронной почты, указанный субъектом ГосСОПКА.

С этого момента взаимодействие считается организованным.

Актуализация сведений об ИР, находящихся в зоне ответственности субъекта ГосСОПКА, или контактных данных лиц, ответственных за взаимодействие, производится в рабочем порядке по электронной почте или с использованием Личного кабинета субъекта ГосСОПКА.

## 6. Каналы взаимодействия

В качестве основных каналов передачи информации в адрес НКЦКИ используются:

– Средства автоматизированного обмена информацией на основе программного интерфейса (посредством API);

– Личный кабинет субъекта ГосСОПКА;

– Электронная почта.

В качестве дополнительных каналов передачи информации используются:

– Почтовые отправления (с приложением электронных носителей информации);

– Телефонная связь.

Получение доступа к личному кабинету возможно только по защищенному каналу, организованному с помощью поддерживаемых типов средств криптографической защиты информации.

Способы организации защищенного канала описаны в документе «Методические рекомендации по организации защищённого обмена информацией с использованием системы личных кабинетов субъектов ГосСОПКА», размещенном на официальном сайте НКЦКИ в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

Защищенный канал с НКЦКИ может быть организован с использованием средств криптографической защиты информации ViPNet производства АО «Инфотекс», АПКШ «Континент» производства ООО «Код Безопасности» или S-Terra производства ООО «С- Терра СиЭсПи».

Поддерживается использование указанных продуктов с уровнем криптографической защиты информации по классу КС3.

**Приложение 1**
**Пример обращения**

**Бланк организации**

Директору НКЦКИ
Скрябину О.В.

Уважаемый Олег Валерьевич!

*«Организация»* выражает согласие осуществлять взаимодействие на основании «Регламента 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-XXX от XX.XX.202Xг, размещенного на официальном сайте НКЦКИ в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

Контактные данные для взаимодействия от *««Организации»*:

*Подразделение по обеспечению информационной безопасности, телефон, email.*

*Руководитель подразделения по обеспечению информационной безопасности, ФИО, телефон, email.*

Взаимодействие будет осуществлять *через Личный кабинет/по электронной почте.*

Одновременно с этим направляем вам сведения об ИР, находящихся в зоне ответственности *««Организации»*.

Приложение: 1. По тексту, CD-диск.

Директор *«Организации»* *ФИО*