УТВЕРЖДАЮ	УТВЕРЖДАЮ
Директор Национального координационного центра по компьютерным инцидентам	*[Руководитель ведомства/организации]*
_____ О.В. Скрябин	_____ инициалы, фамилия
«___»_____ 2025 г.	«___»_____ 2025 г.

РЕГЛАМЕНТ
взаимодействия Национального координационного центра по компьютерным инцидентам и *[наименование ведомства/организации]* при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак

Москва
2025

Оглавление

1. Общие положения. 3

2. Функции участников информационного обмена при осуществлении взаимодействия в области обнаружения, предупреждения и ликвидации последствий КА..... 3

3. Перечень передаваемой информации. 5

4. Каналы взаимодействия. 6

5. Порядок взаимодействия участников информационного обмена. 6

6. Сроки предоставления информации. 7

7. Порядок обмена конфиденциальной информацией …….. 8

8. Контактные данные ……..9

9. Срок действия Регламента, порядок его изменения и расторжения ……9

Приложение 1……...10

1. Общие положения.

1.1 Настоящий Регламент разработан в соответствии со статьей 5 Соглашения о сотрудничестве Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ) и *[наименование ведомства/организации]* в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, и определяет порядок информационного взаимодействия НКЦКИ и *[наименование головного подразделения ведомства/организации]* (далее – участники информационного обмена), уполномоченного выполнятьфункции *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, при решении задач в области обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – КА) на информационные ресурсы (далее – ИР), находящиеся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*.

2. Функции участников информационного обмена при осуществлении взаимодействия в области обнаружения, предупреждения и ликвидации последствий КА.

2.1 В функции НКЦКИ входит:

доведение до *Ведомственного/Корпоративного центра [наименование ведомства/организации]* информации об угрозах информационной безопасности и необходимых мерах по противодействию им;

доведение до *Ведомственного/Корпоративного центра [наименование ведомства/организации]* информации о средствах и способах проведения КА и о методах их обнаружения, предупреждения и противодействия им;

доведение до *Ведомственного/Корпоративного центра [наименование ведомства/организации] информации о признаках КИ;*

оказание содействия в реагировании на компьютерные инциденты (далее – КИ) при обращении *Ведомственного/Корпоративного центра*

[наименование ведомства/организации], обеспечение методической и экспертной поддержки по вопросам реагирования на КИ;

определение состава и форматов предоставляемой *Ведомственным/Корпоративным центром [наименование ведомства/организации]* информации о КИ.

2.2 В функции *Ведомственного/Корпоративного центра [наименование ведомства/организации]* входит:

предоставление в НКЦКИ сведений о составе и характеристиках ИР[1], находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]* в соответствии с составом, структурой и форматом предоставления сведений, определенными НКЦКИ, а также своевременная актуализация таких сведений[2];

ведение перечня организаций и учреждений *[наименование ведомства/организации]*, являющихся субъектами критической информационной инфраструктуры и своевременное информирование НКЦКИ о внесении изменений в данный перечень;

информирование организаций и учреждений *[наименование ведомства/организации]*, в том числе, являющихся субъектами критической информационной инфраструктуры, о рекомендациях, полученных от НКЦКИ по вопросам обнаружения, предупреждения и ликвидации последствий КА;

своевременное предоставление в НКЦКИ и поддержание в актуальном состоянии сведений об ответственных лицах *[наименование ведомства/организации]*, на которых возложены обязанности по взаимодействию с НКЦКИ;

предоставление в НКЦКИ сведений о выявляемых КА и КИ в ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, а также информации

---

[1] Сведения, их состав и характеристики приведены в Приложении 1

2. Сроки предоставления информации представлены в разделе 6 Регламента

о предпринятых мерах и результатах реагирования на такие инциденты и ликвидации последствий КА;

направление в НКЦКИ запросов на содействие в реагировании на КИ;

прием от НКЦКИ информации 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.

3. Перечень передаваемой информации.

3.1 В рамках взаимодействия между участниками информационного обмена передается информация:

о КИ в ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, в соответствии с определенными НКЦКИ форматами, в том числе требующих содействия в реагировании со стороны НКЦКИ;

о признаках КИ в соответствии с форматами, определенными НКЦКИ;

о мерах, предпринятых для локализации КИ в ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, а также о результатах этих мер;

о выявленных угрозах безопасности информации, реализация которых может повлиять на штатное функционирование ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, 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 *Ведомственного/Корпоративного центра [наименование ведомства/организации]*.

Информационные сообщения и запросы, передаваемые по каналам взаимодействия, предусмотренным пунктами 1-3, 5 раздела 4 настоящего Регламента, не должны содержать информацию, составляющую государственную тайну.

Примечание: Формат передаваемых сведений приведен в Приложении 1 настоящего Регламента.

4. Каналы взаимодействия.

При передаче *Ведомственным/Корпоративным центром [наименование ведомства/организации]* информации, указанной в разделе 3 Регламента, в качестве основных каналов передачи информации в адрес НКЦКИ используются:

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

2) Личный кабинет *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, функционирующий в ТИ НКЦКИ.

В качестве дополнительных каналов передачи информации используются:

3) Электронная почта

4) Почтовые отправления.

5) Телефонная связь.

5. Порядок взаимодействия участников информационного обмена.

5.1 Информации о КИ в информационных ресурсах, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, передаваемой в НКЦКИ посредством каналов, указанных в пунктах 1-2 раздела 4 Регламента, в ТИ НКЦКИ присваивается уникальный идентификатор КИ (ID).

5.2 Информация о КИ, передаваемая посредством каналов, указанных в пунктах 3-5 раздела 4 Регламента, учитывается сотрудниками НКЦКИ в ТИ

НКЦКИ, после чего в адрес *Ведомственного/Корпоративного центра [наименование ведомства/организации]* передается ID по тем же каналам.

5.3 При передаче дополнительной информации о КИ в НКЦКИ вне зависимости от канала передачи информации необходимо использовать присвоенный ранее ID.

5.4 При направлении в адрес *Ведомственного/Корпоративного центра [наименование ведомства/организации]* информации о признаках КИ данному уведомлению присваивается идентификатор. В случае подтверждения *Ведомственным/Корпоративным центром [наименование ведомства/организации]* КИ идентификатор уведомления о признаках КИ становится идентификатором КИ.

6. Сроки предоставления информации.

6.1 Информация о КИ, связанном с функционированием значимого объекта критической информационной инфраструктуры, 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 *Ведомственным/Корпоративным центром [наименование ведомства/организации]* в НКЦКИ в срок не позднее 3 часов с момента обнаружения КИ.

6.2 Информация о КИ, связанном с функционированием иных ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]* – в срок не позднее 24 часов с момента его обнаружения.

6.3 Сведения об изменении внешних сетевых реквизитов ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]*, направляются им в адрес НКЦКИ в срок не более 2-х рабочих дней с момента получения информации

данной категории *Ведомственным/Корпоративным центром [наименование ведомства/организации]*.

6.4 Передача сведений об ИР, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации]* осуществляется им в соответствии с составом, структурой и форматом предоставления сведений, определенными НКЦКИ в течении 10 рабочих дней с момента включения (изменения) ИР в зону ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации],* за исключением сведений, указанных в пункте 6.3 настоящего Регламента.

6.5 Подтверждение получения от НКЦКИ информации о признаках КИ, находящихся в зоне ответственности *Ведомственного/Корпоративного центра [наименование ведомства/организации],* направляется в адрес НКЦКИ в срок не более 2-х рабочих дней с момента получения информации данной категории *Ведомственным/Корпоративным центром [наименование ведомства/организации]*.

7. Обмен конфиденциальной информацией

7.1 В настоящем Регламенте под конфиденциальной информацией понимается 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.

7.2 Стороны обязуются сохранять конфиденциальную информацию 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.

7.3 Стороны настоящим соглашаются, что не разгласят и не допустят разглашения конфиденциальной информации третьим лицам без предварительного письменного согласия другой стороны.

7.4 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 Объекты КИИ, вовлеченные в КИ.

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

8. Контактные данные.

Подразделения НКЦКИ и *Ведомственный/Корпоративный центр [наименование ведомства/организации]* при осуществлении взаимодействия используют следующие контактные пункты.

8.1 НКЦКИ:

– сетевой адрес портала НКЦКИ в сети Интернет: cert.gov.ru;

– реквизиты для защищённого подключения: номер сети: 10976;

– адрес портала НКЦКИ: 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;

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

– контактные телефоны: +7 (916) 901-07-42, +7 (495) 621-03-15.

8.2 *Ведомственный/Корпоративный центр [наименование ведомства/организации]*:

9. Срок действия Регламента, порядок его изменения и расторжения.

9.1 Регламент вступает в силу со дня его утверждения и действует бессрочно.

9.2 Регламент может быть расторгнут по взаимному согласию участников информационного обмена, а также по инициативе одной из сторон

с предварительным письменным уведомлением другой стороны не позднее чем за три месяца до дня прекращения его действия.

9.3 НКЦКИ и *Ведомственный/Корпоративный центр [наименование ведомства/организации]* при взаимном согласии вносят в Регламент изменения и дополнения путем утверждения новой редакции Регламента.

С момента утверждения новой редакции Регламента, предыдущая редакция Регламента считается утратившей силу.

Приложение

Таблица 1 - Сведения о субъектах ГосСОПКА

Наименование организации краткое	
Наименование организации полное	
Субъект КИИ	Субъект КИИ
	Не Субъект КИИ
ИНН	
КПП	
Идентификатор ОКОГУ	
Идентификатор ОКОПФ	
ОКВЭД	
Ссылка на официальный сайт (при наличии)	Ссылка на официальный сайт, портал или иной ресурс в сети Интернет.
Тип организации	Федеральный орган государственной власти
	Региональный орган государственной власти
	Центральный банк Российской Федерации
	Некоммерческая организация
	Коммерческая организация
	Местное самоуправление
	Индивидуальный предприниматель
Почтовый адрес организации	Адрес для приема входящей корреспонденции, в том числе абонентский ящик.
Способ взаимодействия с НКЦКИ	Необходимо выбрать один из вариантов: 1) Напрямую. 2) Через аккредитованный Центр ГосСОПКА. В случае выбора второго варианта в строке «Контактные данные для взаимодействия с НКЦКИ» необходимо помимо контактного лица в организации, дополнительно указать наименование Центра ГосСОПКА и его ИНН.

Email-адрес(а) ответственных лиц организации по вопросам обнаружения, предупреждения и реагирования на компьютерные инциденты[3]	На данный email-адрес организации от НКЦКИ будут направляться уведомления о признаках компьютерных инцидентов, уязвимостях и угрозах безопасности информации. Также данный email-адрес организации будет отмечен как «доверенный» для приема с него уведомлений о компьютерных атаках, инцидентах и уязвимостях, выявляемых силами и средствами организации и направляемые по электронной почте в НКЦКИ.
Маршрутизируемые IP-адреса (ipv4) (при наличии)	Указываются маршрутизируемые ipv4-адреса (внутреннюю адресацию указывать не надо), используемые организацией. Перечисляются через запятую поштучно или с масками подсетей. Указание диапазона через дефис недопустимо. В случае смены/дополнения ipv4-адресов, которые используются для обеспечения сетевого взаимодействия информационных ресурсов организации, необходимо обеспечить передачу в установленные Регламентом сроки сведений о новых IP-адресах в НКЦКИ.
Выделенные блоки IP-адресов (при наличии)	Если адреса выделяются динамически, то требуется указать подсеть, из которой выделяются маршрутизируемые IP-адреса. Если неизвестно, то необходимо запросить у провайдера.
Полные доменные имена (FQDN) (при наличии)	Доменные имена второго и выше уровней, ассоциированные, например, с официальным сайтом, электронным почтовым сервером, авторитативными DNS серверами, другими сетевыми сервисами.
Дополнительная значимая информация (при наличии)	Любая дополнительная информация.

[3] Если заключенный договор с аккредитованным Центром ГосСОПКА предусматривает, что взаимодействие НКЦКИ с организацией производится только через указанный Центр ГосСОПКА, поле не заполняется.

Таблица 2 - Сведения о компьютерных инцидентах и атаках

В полях карточки данные могут вносится через запятую или списком. Записи с журналов СЗИ, log-файлы сетевых служб, образцы трафика, электронные образы email-сообщений, образцы вредоносного модуля и другие технические сведения предоставляются в отдельном файле.

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	DDoS-атака
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь

	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Неудачные попытки авторизации
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости

	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	

IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Попытки внедрения ВПО
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости

	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	

URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы [Центр управления ВПО]	
IPv4-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv4-адрес вредоносной системы [Источник распространения ВПО]	
IPv4-адрес вредоносной системы [Тип неопределен]	
IPv6-адрес вредоносной системы [Центр управления ВПО]	
IPv6-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv6-адрес вредоносной системы [Источник распространения ВПО]	
IPv6-адрес вредоносной системы [Тип неопределен]	
Доменное имя вредоносной системы [Центр управления ВПО]	
Доменное имя вредоносной системы [Элемент инфраструктуры ВПО]	
Доменное имя вредоносной системы [Источник распространения ВПО]	
Доменное имя вредоносной системы [Тип неопределен]	
URI-адрес вредоносной системы [Центр управления ВПО]	
URI-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
URI-адрес вредоносной системы [Источник распространения ВПО]	

URI-адрес вредоносной системы [Тип неопределен]	
Email-адрес вредоносного объекта	
Хеш-сумма вредоносного модуля (1)	
Вердикт антивирусного средства (в случае сработки) (1)	
Хеш-сумма вредоносного модуля (2)	
Вердикт антивирусного средства (в случае сработки) (2)	
Хеш-сумма вредоносного модуля (3)	
Вердикт антивирусного средства (в случае сработки) (3)	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Попытки эксплуатации уязвимости
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости

Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	

IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Email-адрес вредоносного объекта	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Публикация мошеннической информации
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости

	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	

IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Сетевое сканирование
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости

Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	

Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	Социальная инженерия
Статус реагирования	Меры приняты, атака локализована
	Проводятся мероприятия по локализации компьютерной атаки
	Возобновлены мероприятия по локализации компьютерной атаки
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Информация о контролируемом ресурсе, на который направлена КА	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости

Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	

Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Email-адрес вредоносного объекта	
Описание используемых уязвимостей	
Дополнительные значимые сведения о компьютерной атаке (в свободной форме)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Использование контролируемого ресурса для проведения атак
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Локация	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес вредоносной системы [Центр управления ВПО]	
IPv4-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv4-адрес вредоносной системы [Источник распространения ВПО]	
IPv4-адрес вредоносной системы [Тип неопределен]	
IPv6-адрес вредоносной системы [Центр управления ВПО]	
IPv6-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv6-адрес вредоносной системы [Источник распространения ВПО]	
IPv6-адрес вредоносной системы [Тип неопределен]	
Доменное имя вредоносной системы [Центр управления ВПО]	
Доменное имя вредоносной системы [Элемент инфраструктуры ВПО]	
Доменное имя вредоносной системы [Источник распространения ВПО]	
Доменное имя вредоносной системы [Тип неопределен]	
URI-адрес вредоносной системы [Центр управления ВПО]	
URI-адрес вредоносной системы [Элемент инфраструктуры ВПО]	

URI-адрес вредоносной системы [Источник распространения ВПО]	
URI-адрес вредоносной системы [Тип неопределен]	
Email-адрес вредоносного объекта	
Хеш-сумма вредоносного модуля (1)	
Вердикт антивирусного средства (в случае сработки) (1)	
Хеш-сумма вредоносного модуля (2)	
Вердикт антивирусного средства (в случае сработки) (2)	
Хеш-сумма вредоносного модуля (3)	
Вердикт антивирусного средства (в случае сработки) (3)	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Замедление работы ресурса в результате DDoS-атаки
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Заражение ВПО
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы [Центр управления ВПО]	
IPv4-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv4-адрес вредоносной системы [Источник распространения ВПО]	
IPv4-адрес вредоносной системы [Тип неопределен]	
IPv6-адрес вредоносной системы [Центр управления ВПО]	
IPv6-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
IPv6-адрес вредоносной системы [Источник распространения ВПО]	
IPv6-адрес вредоносной системы [Тип неопределен]	
Доменное имя вредоносной системы [Центр управления ВПО]	

Доменное имя вредоносной системы [Элемент инфраструктуры ВПО]	
Доменное имя вредоносной системы [Источник распространения ВПО]	
Доменное имя вредоносной системы [Тип неопределен]	
URI-адрес вредоносной системы [Центр управления ВПО]	
URI-адрес вредоносной системы [Элемент инфраструктуры ВПО]	
URI-адрес вредоносной системы [Источник распространения ВПО]	
URI-адрес вредоносной системы [Тип неопределен]	
Email-адрес вредоносного объекта	
Хеш-сумма вредоносного модуля (1)	
Вердикт антивирусного средства (в случае сработки) (1)	
Хеш-сумма вредоносного модуля (2)	
Вердикт антивирусного средства (в случае сработки) (2)	
Хеш-сумма вредоносного модуля (3)	
Вердикт антивирусного средства (в случае сработки) (3)	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Захват сетевого трафика
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует
	Влияние на доступность: Высокое

	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да

	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
AS-Path до атакованной Автономной системы (ASN)	
Технические сведения о вредоносной системе	
Номер подставной Автономной системы (ASN)	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Компрометация учетной записи
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Несанкционированное изменение информации
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Несанкционированное разглашение информации
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Email-адрес вредоносного объекта	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Публикация на ресурсе запрещенной законодательством РФ информации
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует

	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует
Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование

Наличие подключения к сети Интернет	Да
	Нет
Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Описание используемых уязвимостей	

Рег.номер уведомления	Предоставляет НКЦКИ
Дата и время регистрации уведомления	Предоставляет НКЦКИ
Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Успешная эксплуатация уязвимости
Статус реагирования	Меры приняты, инцидент исчерпан
	Проводятся мероприятия по реагированию на инцидент
	Возобновлены мероприятия по реагированию на инцидент
Необходимость привлечения сил ГосСОПКА	Да
	Нет
Краткое описание события ИБ	
Сведения о средстве или способе выявления	
Дата и время выявления	
Дата и время завершения	
Ограничительный маркер TLP	TLP:WHITE
	TLP:GREEN
	TLP:AMBER
	TLP:RED
Владелец информационного ресурса	
Заявитель	
Оценка последствий КИ	Влияние на конфиденциальность: Высокое
	Влияние на конфиденциальность: Низкое
	Влияние на конфиденциальность: Отсутствует
	Влияние на целостность: Высокое
	Влияние на целостность: Низкое
	Влияние на целостность: Отсутствует
	Влияние на доступность: Высокое
	Влияние на доступность: Низкое
	Влияние на доступность: Отсутствует

Краткое описание иной формы последствий компьютерного инцидента	
Информация о контролируемом ресурсе, на котором выявлен КИ	
Наименование	
Информация о категорировании ОКИИ	Информационный ресурс не является объектом КИИ
	Объект КИИ без категории значимости
	Объект КИИ третьей категории значимости
	Объект КИИ второй категории значимости
	Объект КИИ первой категории значимости
	Информационный ресурс не является объектом КИИ
Сфера функционирования	Здравоохранение
	Наука
	Транспорт
	Связь
	Банковская сфера и иные сферы финансового рынка
	Энергетика и Топливно-энергетический комплекс
	Атомная энергия
	Оборонная промышленность
	Ракетно-космическая промышленность
	Горнодобывающая промышленность
	Металлургическая промышленность
	Химическая промышленность
	СМИ
	Государственная/муниципальная власть
	Образование
Наличие подключения к сети Интернет	Да
	Нет

Местоположение контролируемого ресурса	
Страна/Регион	
Населенный пункт или геокоординаты	
Технические сведения о контролируемом ресурсе	
IPv4-адрес (маршрутизируемый) атакованного ресурса	
IPv6-адрес (маршрутизируемый) атакованного ресурса	
Доменное имя атакованного ресурса	
URI-адрес атакованного ресурса	
Email-адрес атакованного ресурса	
Атакованная сетевая служба и порт/протокол	
Технические сведения о вредоносной системе	
IPv4-адрес вредоносной системы	
IPv6-адрес вредоносной системы	
Доменное имя вредоносной системы	
URI-адрес вредоносной системы	
Email-адрес вредоносного объекта	
Описание используемых уязвимостей	