



Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

Федеральное государственное автономное образовательное
учреждение высшего образования «Российский государственный
университет нефти и газа (национальный исследовательский
университет) имени И.М. Губкина»

Факультет комплексной безопасности ТЭК



Приказ ФСБ России от 24.07.2018 N 367

Выполнил: Лазорин Д.С., группа КС-21-04.



Полное наименование

«Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».



Кого касается

1. Предприятие, которому принадлежит объект критической информационной инфраструктуры (КИИ).
2. Любое другое предприятие, имеющее отношение к инциденту на объекте КИИ



Когда применяется

Произошел инцидент с объектом КИИ
(кибератака, сбой, утечка информации,
нарушена связь).



Самое главное

Предприятие, владеющее объектом КИИ, должно передавать в ГосСОПКУ информацию о компьютерном инциденте в течение 24 часов с момента его обнаружения. Информация передается через НКЦИ в определенном формате



Сокращения и термины, используемые в НПА

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



Сокращения и термины, используемые в НПА

Объект КИИ – информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере: здравоохранения; науки; транспорта; связи; энергетики; банковской и иных сферах финансового рынка; топливно-энергетического комплекса; атомной энергии; оборонной и ракетно-космической промышленности; горнодобывающей, металлургической и химической промышленности.



Сокращения и термины, используемые в НПА

Значимый объект КИИ – объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ.



Сокращения и термины, используемые в НПА

Субъект КИИ – организация является субъектом КИИ, если виды деятельности, прописанные в уставных документах данной организации, относятся к области: здравоохранения; науки; транспорта; связи; энергетики; банковской и иных сфер финансового рынка; топливно-энергетического комплекса; атомной энергии; оборонной и ракетно-космической промышленности; горнодобывающей, металлургической и химической промышленности.



Сокращения и термины, используемые в НПА

НКЦИ – национальный координационный центр по компьютерным инцидентам. Координирует деятельность субъектов КИИ РФ, связанную с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагирования на компьютерные инциденты. Сайт: <https://cert.gov.ru/>



Сокращения и термины, используемые в НПА

ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Единый территориально распределенный комплекс, включающий силы и программно-технические средства обнаружения, предупреждения и ликвидации последствий компьютерных атак.



Сокращения и термины, используемые в НПА

ГосСОПКА предназначена для контроля безопасности КИИ в Российской Федерации и в дипломатических представительствах страны за рубежом. В системе собирается информация о компьютерных атаках и инцидентах, получаемая от субъектов КИИ. Частью ГосСОПКА является НКЦКИ — Национальный координационный центр по компьютерным инцидентам.



Сокращения и термины, используемые в НПА

ГосСОПКА предназначена для контроля безопасности КИИ в Российской Федерации и в дипломатических представительствах страны за рубежом. В системе собирается информация о компьютерных атаках и инцидентах, получаемая от субъектов КИИ. Частью ГосСОПКА является НКЦКИ — Национальный координационный центр по компьютерным инцидентам.



Краткое изложение

Приказ утверждает перечень информации, предоставляемой в ГосСОПКА, а также порядок ее предоставления. В ГосСОПКА предоставляется следующая информация.



Кем предоставляется

Федеральным органом исполнительной власти (ФОИВ), уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации



Сроки предоставления

Передается не реже раза в месяц и не позже месяца с момента: включения объекта КИИ в реестр; изменения категории значимости объекта; получения информации об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости; исключения объекта КИИ из реестра; составления акта проверки по итогам осуществления государственного контроля, в котором содержится информация о нарушениях.



Предоставляемая информация

1. Информация, содержащаяся в реестре значимых объектов КИИ.
2. Информация об отсутствии необходимости присвоения объекту КИИ категории значимости.
3. Информация об исключении объекта КИИ из реестра, а также об изменении категории его значимости.
4. Информация по итогам проведения государственного контроля.



Как передается

Направляется
определенных
(ФОИВом).

в НКЦКИ в
уполномоченным

форматах,
органом



Кем предоставляется
Субъектами КИИ через НКЦКИ.



Сроки предоставления

Не позднее 24 часов с момента обнаружения компьютерного инцидента.



Предоставляемая информация

Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ: дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошел компьютерный инцидент; наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;



Предоставляемая информация

связь с другими компьютерными инцидентами (при наличии); состав технических параметров компьютерного инцидента; последствия компьютерного инцидента. НКЦКИ уведомляет субъект КИИ о получении информации не позднее 24 часов с момента ее получения.



Как передается

Направляется в НКЦКИ в определенных форматах. Если отсутствует подключение к технической инфраструктуре НКЦКИ, информация направляется по почте, факсу или электронной связи по контактам на сайте <https://cert.gov.ru>.



Кем предоставляется

Субъектами КИИ и иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными.



Сроки предоставления

Достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.



Предоставляемая информация

Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты



Как передается

С использованием технической инфраструктуры НКЦКИ или посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте <https://cert.gov.ru/>.



Список использованных источников

1. Приказ № 367 // Kaspersky URL:
<https://regulhub.kaspersky.ru/decrees/prikaz-367>
(дата обращения: 02.10.2025).