НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ПРИКАЗ

14 ИЮЛ 2026 **Москва** **№ 2**

О совершенствовании деятельности по организации взаимодействия Национального координационного центра по компьютерным инцидентам с субъектами критической информационной инфраструктуры, центрами ГосСОПКА и органами (организациями)

В целях совершенствования деятельности по организации взаимодействия Национального координационного центра по компьютерным инцидентам с субъектами критической информационной инфраструктуры, центрами ГосСОПКА и органами (организациями) и в соответствии с пунктами 4.9 и 4.10 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 (зарегистрирован в Минюсте России, регистрационный № 52109 от 6 сентября 2018 г.) с изменениями, внесенными приказом ФСБ России от 24 декабря 2025 г. № 540 (зарегистрирован в Минюсте России, регистрационный № 84777 от 25 декабря 2025 г.),

П Р И К А З Ы В А Ю :

1. Определить:

1.1. Формат представления информации о компьютерных атаках в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и состав технических параметров компьютерной атаки, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение 1).

1.2. Формат представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и состав технических параметров компьютерного инцидента, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение 2).

2. Довести определенные форматы и составы технических параметров до субъектов критической информационной инфраструктуры Российской Федерации, аккредитованных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также органов и организаций, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», путем их публикации на официальном сайте Национального координационного центра по компьютерным инцидентам в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru/».

3. Установить, что Исходные данные для определения типа компьютерной атаки (утвержденные Директором Национального

координационного центра по компьютерным инцидентам от 8 июля 2026 г.), а также описание правил и протоколов автоматизированного взаимодействия технической инфраструктуры Национального координационного центра по компьютерным инцидентам с системами субъектов критической информационной инфраструктуры Российской Федерации, аккредитованных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, органов и организаций, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также иных субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, размещаются на официальном сайте Национального координационного центра по компьютерным инцидентам в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru/».

Директор О.В. Скрябин

Приложение 1
к приказу НКЦКИ
от 14 июля 2026 г.
№ 2

Формат представления информации о компьютерных атаках в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и состав технических параметров компьютерной атаки, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Наименование поля	**Обязательность заполнения**	**Справочные значения (при наличии)**	**Правила заполнения полей**
Категория	Обязательно	Уведомление о компьютерной атаке	Строго справочное значение. Внесение иных значений недопустимо.
Тип компьютерной атаки	Обязательно	DDoS-атака Неудачные попытки авторизации Попытки внедрения вредоносного программного обеспечения (ВПО) Попытки эксплуатации уязвимости Публикация мошеннической информации Сетевое сканирование Социальная инженерия	Строго справочное значение. Внесение иных значений недопустимо.
Информация о владельце защищаемого информационного ресурса и заявителе			
Сокращенное наименование организации владельца информационного ресурса	Обязательно		Заполняется в соответствии с официальным наименованием.
Полное наименование организации владельца информационного ресурса	Обязательно		Заполняется в соответствии с регистрацией в ФНС.
ИНН	Обязательно		Заполняется только в виде цифр. 10 цифр для юридических лиц, 12 цифр для ИП.

КПП	Обязательно (При отсутствии указывается значение «000000000»)		Заполняется только в виде цифр. Равен 9 знакам.
ОГРН	Обязательно		Заполняется только в виде цифр. Равен 13 знакам.
Заявитель	Обязательно		Заполняется в случае, если наименование заявителя отличается от владельца информационного ресурса (владелец – субъект КИИ, заявитель – Центр ГосСОПКА). Заполняется сокращенное наименование организации в соответствии с официальным наименованием.
Информация о выявленной компьютерной атаке			
Краткое описание компьютерной атаки	Обязательно		Заполняется текстом в свободной форме.
Необходимость привлечения сил ФСБ России	Обязательно	— true — false	Поле типа Boolean. Если необходима помощь ФСБ России в реагировании на событие, то необходимо установить значение true.
Ограничительный маркер TLP	Обязательно	— TLP:WHITE — TLP:RED — TLP:GREEN — TLP:AMBER	Строго справочное значение. Внесение иных значений недопустимо.
Сведения о средстве или способе выявления	Не обязательно		Заполняется текстом в свободной форме.
Дата и время выявления	Обязательно		Дата должна быть заполнена в следующем формате: YYYY-MM DDTH:M:SGMT, где: • YYYY – год, MM – месяц, DD – день • H – часы, M – минуты, S – секунды • GMT – часовой пояс.
Дата и время завершения	Не обязательно		Дата должна быть заполнена в следующем формате: YYYY-MM DDTH:M:SGMT, где: • YYYY – год, MM – месяц, DD – день • H – часы, M – минуты, S – секунды • GMT – часовой пояс.
Информация о защищаемом ресурсе			
Наименование	Обязательно		Указывается наименование атакованного объекта. Заполняется текстом в свободной форме.

Информация о категорировании	Обязательно	— 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	Строго справочное значение. Внесение иных значений недопустимо.
Сфера функционирования	Обязательно	— Здравоохранение — Наука — Транспорт — Связь — Энергетика — Государственная регистрация права на недвижимое имущество и сделок с ним — Банковская сфера и иные сферы финансового рынка — Топливно-энергетический комплекс — Атомная энергетика — Оборонная промышленность — Ракетно-космическая промышленность — Горнодобывающая промышленность — Металлургическая промышленность; — Химическая промышленность — СМИ	Строго справочное значение. Внесение иных значений недопустимо.

		— Государственная/муниципальная власть — Образование — Иная	
Наличие подключения к сети Интернет	Обязательно	— true — false	Поле типа Boolean. Если атакованный ресурс подключен к сети Интернет, то необходимо установить значение true.
Местоположение контролируемого ресурса			
Локация	Обязательно		Указывается информация о местонахождении атакованного ресурса, а не местонахождении головной организации. В поле необходимо указать геокод первого и второго уровня административно территориального деления территории всех стран согласно стандарта ISO-3166-2. Например, для Новосибирской области согласно ISO-3166-2 установлен код " RU NVS".
Населенный пункт или геокоординаты	Не обязательно		В этом поле детализируется точно до города/поселка/села или любого другого населенного пункта. В случае, если указать населенный пункт невозможно, допустимо указание геокоординат.
Технические параметры защищаемого информационного ресурса			
IPv4-адрес	Направляется по мере определения		Заполняется в в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Может быть указано несколько значений. Описание сети через маску недопустимо.

IPv6-адрес	Направляется по мере определения		Заполняется как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (::). Может быть указано несколько значений.
Доменное имя	Направляется по мере определения		Заполняется согласно общепринятым правилам написания доменных имен. Может быть указано несколько значений. Указание гиперссылками недопустимо.
URI-адрес	Направляется по мере определения		Заполняется согласно общепринятым правилам написания URI-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо.
Email-адрес атакованного ресурса	Направляется по мере определения		Заполняется согласно общепринятым правилам написания Email-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо.
Сетевая служба и порт/протокол	Направляется по мере определения		Поле типа объект, в которое записываются два значения: сетевая служба и порт/протокол. Может быть указано несколько значений.
AS-Path до атакованной Автономной системы (ASN)	Направляется по мере определения		Заполняется согласно общепринятым правилам написания AS-Path.
Технические параметры выявленной вредоносной активности			
IPv4-адрес вредоносной системы	Направляется по мере выявления		Заполняется в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Может быть указано несколько значений. Описание сети через маску недопустимо.

			Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
IPv6-адрес вредоносной системы	Направляется по мере выявления		Заполняется как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (::). Может быть указано несколько значений. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
Доменное имя вредоносной системы	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания доменных имен. Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
URI-адрес вредоносной системы	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания URI-адресов.

			Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
Email-адрес вредоносного объекта	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания Email-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
Хеш-сумма вредоносного модуля	Направляется по мере выявления		В поле указывается один из следующих форматов контрольной суммы: — sha256; — sha512; — sha1; — md5; — GOST-R-34.11-2018; — GOST-R-34.11-2012; — GOST-R-34.11-94. Может быть указано несколько значений.
Описание используемых уязвимостей	Направляется по мере выявления		Заполняется текстом в свободной форме. Может быть указано несколько значений.
Номер подставной Автономной системы (ASN)	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания номера ASN.
Наименование AS	Направляется по мере выявления		Заполняется текстом в свободной форме.

Наименование LIR	Направляется по мере выявления		Заполняется текстом в свободной форме.
Записи с журналов средств защиты информации, log-файлы сетевых служб, образцы трафика, электронные образы email-сообщений	Направляется по мере выявления		Предоставляются в отдельном файле.

Приложение 2
к приказу НКЦКИ
от 14 июля 2026 г.
№ 2

Формат представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и состав технических параметров компьютерного инцидента, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Наименование поля	**Обязательность заполнения**	**Справочные значения (при наличии)**	**Правила заполнения полей**
Категория	Обязательно	Уведомление о компьютерном инциденте	Строго справочное значение. Внесение иных значений недопустимо.
Тип компьютерного инцидента	Обязательно	Использование контролируемого ресурса для проведения атак Замедление работы ресурса в результате DDoS-атаки Заражение ВПО Захват сетевого трафика Компрометация учетной записи Несанкционированное изменение информации Несанкционированное разглашение информации Публикация на ресурсе запрещенной законодательством РФ информации Событие не связано с компьютерной атакой Успешная эксплуатация уязвимости	Строго справочное значение. Внесение иных значений недопустимо.
Информация о владельце защищаемого информационного ресурса и заявителе			

Сокращенное наименование организации владельца информационного ресурса	Обязательно		Заполняется в том виде, в котором было передано сокращенное наименование организации при организации взаимодействия с НКЦКИ.
Полное наименование организации владельца информационного ресурса	Обязательно		Заполняется в соответствии с регистрацией в ФНС.
ИНН	Обязательно		Заполняется только в виде цифр. 10 цифр для юридических лиц, 12 цифр для ИП.
КПП	Обязательно (При отсутствии указывается значение «000000000»)		Заполняется только в виде цифр. Равен 9 знакам.
ОГРН	Обязательно		Заполняется только в виде цифр. Равен 13 знакам.
Заявитель	Обязательно		Заполняется в случае, если наименование заявителя отличается от владельца информационного ресурса (владелец – субъект КИИ, заявитель – Центр ГосСОПКА). Заполняется сокращенное наименование организации в том виде, в котором было передано сокращенное наименование организации при организации взаимодействия с НКЦКИ.
Информация о выявленной компьютерном инциденте			
Краткое описание события ИБ	Обязательно		Заполняется текстом в свободной форме.
Статус реагирования	Обязательно	— Меры приняты — Проводятся мероприятия по реагированию — Возобновлены мероприятия по реагированию	Строго справочное значение. Внесение иных значений недопустимо.

Привлеченные силы реагирования	Обязательно		Текстовое поле. Требуется указать наименование привлеченной организации. Должно соответствовать перечню Центров ГосСОПКА на сайте gossopka.ru. Если реагирование осуществлялось самостоятельно, необходимо указать, что привлечение сторонних организаций не требуется.
Необходимость привлечения сил ФСБ России	Обязательно	— true — false	Поле типа Boolean. Если необходима помощь ФСБ России в реагировании на событие, то необходимо установить значение true.
Сведения о средстве или способе выявления	Не обязательно		Заполняется текстом в свободной форме.
Ограничительный маркер TLP	Обязательно	— TLP:WHITE — TLP:RED — TLP:GREEN — TLP:AMBER	Строго справочное значение. Внесение иных значений недопустимо.
Дата и время выявления	Обязательно		Дата должна быть заполнена в следующем формате: YYYY-MM DDTH:M:SGMT, где: • YYYY – год, MM – месяц, DD – день • H – часы, M – минуты, S – секунды • GMT – часовой пояс.
Дата и время завершения	Не обязательно		Дата должна быть заполнена в следующем формате: YYYY-MM DDTH:M:SGMT, где: • YYYY – год, MM – месяц, DD – день • H – часы, M – минуты, S – секунды • GMT – часовой пояс.
Влияние на конфиденциальность	Не обязательно	— Высокое — Низкое — Отсутствует	Строго справочное значение. Внесение иных значений недопустимо.
Влияние на целостность	Не обязательно	— Высокое — Низкое — Отсутствует	Строго справочное значение. Внесение иных значений недопустимо.
Влияние на доступность	Не обязательно	— Высокое — Низкое — Отсутствует	Строго справочное значение Внесение иных значений недопустимо.
Краткое описание иной формы последствий компьютерного инцидента	Не обязательно		Поле заполняется в свободной форме.
Утечка ПДн	Не обязательно	— true — false	Поле типа Boolean.

			Если инцидент повлек также утечку ПДн, то необходимо установить значение true.
Сведения об утечке персональных данных			
Адрес оператора	Обязательно, если заполнено поле Утечка ПДн		Адрес заполняется в формате: Индекс, Регион, Населенный пункт, Улица, Дом
Адрес электронной почты для отправки информации об уведомлении	Обязательно, если заполнено поле Утечка ПДн		Заполняется согласно общепринятым правилам написания Email-адресов.
Предполагаемые причины, повлекшие нарушение прав субъектов ПД	Обязательно, если заполнено поле Утечка ПДн		Поле заполняется в свободной форме.
Характеристики персональных данных	Обязательно, если заполнено поле Утечка ПДн		Поле заполняется в свободной форме.
Предполагаемый вред, нанесенный правам субъектов ПД	Обязательно, если заполнено поле Утечка ПДн		Поле заполняется в свободной форме.
Принятые меры по устранению последствий инцидента	Не обязательно		Поле заполняется в свободной форме.
Дополнительный сведения	Не обязательно		Поле заполняется в свободной форме.
Информация о результатах внутреннего расследования инцидента	Не обязательно		Поле заполняется в свободной форме.
Информация о защищаемом ресурсе			
Наименование	Обязательно		Указывается наименование атакованного объекта. Заполняется текстом в свободной форме.

Информация о категорировании	Обязательно	— 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	Строго справочное значение. Внесение иных значений недопустимо.
Сфера функционирования	Обязательно	— Здравоохранение — Наука — Транспорт — Связь — Энергетика — Государственная регистрация права на недвижимое имущество и сделок с ним — Банковская сфера и иные сферы финансового рынка — Топливно-энергетический комплекс — Атомная энергетика — Оборонная промышленность — Ракетно-космическая промышленность — Горнодобывающая промышленность — Металлургическая промышленность; — Химическая промышленность — СМИ — Государственная/муниципальная власть — Образование — Иная	— Строго справочное значение. Внесение иных значений недопустимо.
Наличие подключения к сети Интернет	Обязательно	Boolean: — true — false	Поле типа Boolean. Если атакованный ресурс подключен к сети Интернет, то

			необходимо установить значение true.
Местоположение контролируемого ресурса			
Локация	Обязательно		Указывается информация о местонахождении атакованного ресурса, а не местонахождении головной организации. В поле необходимо указать геокод первого и второго уровня административно территориального деления территории всех стран согласно стандарта ISO-3166-2. Например, для Новосибирской области согласно ISO-3166-2 установлен код " RU NVS".
Населенный пункт или геокоординаты	Не обязательно		В этом поле детализируется точно до города/поселка/села или любого другого населенного пункта. В случае, если указать населенный пункт невозможно, допустимо указание геокоординат.
Технические параметры защищаемого информационного ресурса			
IPv4-адрес	Направляется по мере определения		Заполняется в в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Может быть указано несколько значений. Описание сети через маску недопустимо.
IPv6-адрес	Направляется по мере определения		Заполняется как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (::). Может быть указано несколько значений.
Доменное имя	Направляется по мере определения		Заполняется согласно общепринятым правилам написания доменных имен. Может быть указано несколько значений. Указание гиперссылками недопустимо.
URI-адрес	Направляется по мере определения		Заполняется согласно общепринятым правилам написания URI-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо.
Email-адрес атакованного ресурса	Направляется по мере определения		Заполняется согласно общепринятым правилам написания Email-адресов. Может быть указано несколько значений.

			Указание гиперссылками недопустимо.
Сетевая служба и порт/протокол	Направляется по мере определения		Поле типа объект, в которое записываются два значения: сетевая служба и порт/протокол. Может быть указано несколько значений.
AS-Path до атакованной Автономной системы (ASN)	Направляется по мере определения		Заполняется согласно общепринятым правилам написания AS-Path.
Технические параметры выявленной вредоносной активности			
IPv4-адрес вредоносной системы	Направляется по мере выявления		Заполняется в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Может быть указано несколько значений. Описание сети через маску недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
IPv6-адрес вредоносной системы	Направляется по мере выявления		Заполняется как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (::). Может быть указано несколько значений. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносны

			индикаторы каждый с новой строки без разделительных знаков.
Доменное имя вредоносной системы	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания доменных имен. Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
URI-адрес вредоносной системы	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания URI-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.
Email-адрес вредоносного объекта	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания Email-адресов. Может быть указано несколько значений. Указание гиперссылками недопустимо. Можно указать не больше 30 индикаторов. Если индикаторов больше 30, то сведения о них предоставляются в приложении в текстовом файле. Файл должен иметь название indicators.txt и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.

Хеш-сумма вредоносного модуля	Направляется по мере выявления		В поле указывается один из следующих форматов контрольной суммы: — sha256; — sha512; — sha1; — md5; — GOST-R-34.11-2018; — GOST-R-34.11-2012; — GOST-R-34.11-94. Может быть указано несколько значений.
Описание используемых уязвимостей	Направляется по мере выявления		Заполняется текстом в свободной форме. Может быть указано несколько значений.
Номер подставной Автономной системы (ASN)	Направляется по мере выявления		Заполняется согласно общепринятым правилам написания номера ASN.
Наименование AS	Направляется по мере выявления		Заполняется текстом в свободной форме.
Наименование LIR	Направляется по мере выявления		Заполняется текстом в свободной форме.
Записи с журналов средств защиты информации, log-файлы сетевых служб, образцы трафика, электронные образы email-сообщений	Направляется по мере выявления		Предоставляются в отдельном файле.