Национальный координационный центр по компьютерным инцидентам

НКЦКИ

Инструкция по формированию электронного письма уведомления о компьютерном инциденте или атаке

Версия документа: 2.0

Дата документа: 05.05.2023

г. Москва, 2023

Содержание

1. Аннотация 3
2. Принятые сокращения 3
3. Правила направления Уведомления по ЭП 3
   3.1. Выбор шаблона Уведомления по ЭП 3
   3.2. Заполнение полей шаблона Уведомления по ЭП 5
4. Шаблоны Уведомлений по ЭП 17
   4.1. Шаблоны Уведомлений о компьютерном инциденте 17
   4.1.1. Шаблон Использование контролируемого ресурса для проведения атак 17
   4.1.2. Шаблон Замедление работы ресурса в результате DDoS-атаки 18
   4.1.3. Шаблон Заражение ВПО 19
   4.1.4. Шаблон Захват сетевого трафика 20
   4.1.5. Шаблон Компрометация учетной записи 21
   4.1.6. Шаблон Несанкционированное изменение информации 23
   4.1.7. Шаблон Несанкционированное разглашение информации 24
   4.1.8. Шаблон Публикация на ресурсе запрещенной законодательством РФ информации 25
   4.1.9. Шаблон Успешная эксплуатация уязвимости 26
   4.1.10. Шаблон Событие не связано с компьютерной атакой 27
   4.2. Шаблоны Уведомлений о компьютерной атаке 28
   4.2.1. Шаблон DDoS-атака 28
   4.2.2. Шаблон Неудачные попытки авторизации 29
   4.2.3. Шаблон Попытки внедрения ВПО 30
   4.2.4. Шаблон Попытки эксплуатации уязвимости 31
   4.2.5. Шаблон Публикация мошеннической информации 32
   4.2.6. Шаблон Сетевое сканирование 33
   4.2.7. Шаблон Социальная инженерия 34

1. Аннотация

Уведомления о компьютерных инцидентах и компьютерных атаках должны направляться в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – ГосСОПКА) согласно установленным Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ) форматам. В настоящей Инструкции приведены правила формирования Уведомлений о компьютерных инцидентах и компьютерных атаках, направляемых на электронную почту НКЦКИ: incident@cert.gov.ru (далее – Уведомления по ЭП).

2. Принятые сокращения

Сокращение	Расшифровка
ВПО	Вредоносное программное обеспечение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
ИБ	Информационная безопасность
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
ЭП	Электронная почта

3. Правила направления Уведомления по ЭП

Формирование Уведомления по ЭП включает в себя два этапа:

1. Выбор шаблона Уведомления по ЭП
2. Заполнение полей шаблона Уведомления по ЭП
3. Текст уведомления в тегах заполняется в теле письма. Во вложении могут быть добавлены дополнительные сведения в файлах.
4. Скриншоты, картинки и иные цифровые доказательства нельзя размещать в теле письма, необходимо добавлять отдельно прикрепленными файлами.

3.1. Выбор шаблона Уведомления по ЭП

Все Уведомления по ЭП разделяются на 3 категории:

- Уведомление о компьютерном инциденте;
- Уведомление о компьютерной атаке.

Каждой категории соответствует набор определённых типов событий информационной безопасности (далее – ИБ). Для каждого типа события ИБ установлен свой набор полей, которые необходимо направить на электронную почту НКЦКИ. Этот набор полей представлен в настоящей Инструкции в виде шаблонов для каждого типа события ИБ. Перечень шаблонов представлен в таблице ниже. Для перехода к шаблону и его копирования необходимо кликнуть по наименованию типа события ИБ в таблице.

Категория	Типы событий ИБ
Уведомление о компьютерном инциденте	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
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия

Шаблоны состоят из набора тегов, обозначаемых латинскими наименованиями. В тегах шаблона необходимо заменить *** на значения, которые присущи тому или иному тегу. Правила заполнения полей шаблона представлены в разделе 3.2 настоящей Инструкции.

При использовании шаблона обратите внимание на блоки:

- Технические сведения об атакованном ресурсе;
- Технические сведения о вредоносной системе.

Перечисленные блоки необходимо включить в Уведомление по ЭП, если в поле **Наличие подключения к сети Интернет** в блоке ***Общие сведения о контролируемом ресурсе*** выставлено значение true (т.е. если у контролируемого ресурса имеется подключение к сети Интернет). В случае, если у контролируемого ресурса отсутствует подключение к сети Интернет перечисленные блоки необходимо удалить из шаблона направляемого электронного письма.

Блок Сведения об утечке персональных данных необходимо включить в Уведомление по ЭП, если в поле **Утечка ПДн** в блоке ***Общие сведения*** выставлено значение true. Данный блок может быт заполнен только для следующих типов события ИБ:

- Заражение ВПО;
- Компрометация учетной записи;
- Несанкционированное разглашение информации;
- Успешная эксплуатация уязвимости;
- Событие не связано с компьютерной атакой.

Также обратите внимание, что если у вас отсутствуют сведения для заполнения не обязательного поля, то это поле необходимо удалить из шаблона направляемого электронного письма. **Поля со звездочками не отправлять!**

3.2. Заполнение полей шаблона Уведомления по ЭП

Шаблоны Уведомлений по ЭП в зависимости от категории и типа события ИБ могут включать в себя перечень полей, представленных в таблице ниже. В таблице ниже указаны основные характеристики полей (обязательное или не обязательное для заполнения, необходимость заполнения на основе справочника), а также примеры заполнения полей.

В блоке Технические сведения о вредоносной системе можно указать не больше 30 индикаторов. Если индикаторов больше блок **Технические сведения о вредоносной системе** в тексте письма необходимо удалить из шаблона. Сведения о них предоставляются в приложении к письму в текстовом файле. Файл должен иметь название **indicators.txt** и содержать вредоносные индикаторы каждый с новой строки без разделительных знаков.

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
Общие сведения				
Наименование организации владельца информационного ресурса	[company_name: ***]	❗ Обязательно	Наименование необходимо заполнять в том виде, в котором было передано сокращенное наименование организации в НКЦКИ при подключении к ГосСОПКА для информационного обмена по почте	[company_name: АО «Ромашка»]
Статус реагирования	[activity_status: ***]	❗ Обязательно	• Меры приняты • Проводятся мероприятия по реагированию • Возобновлены мероприятия по реагированию	[activity_status: Проводятся мероприятия по реагированию]
Необходимость привлечения сил ГосСОПКА	[assistance: ***]	❗ Обязательно	Boolean: • true • false	[assistance: true]
Краткое описание события ИБ	[event_description: ***]	❗ Обязательно	Поле заполняется в свободной форме	[event_description: На хосте выявлен вирус BlackEnergy]
Сведения о средстве или способе выявления	[detection_tool: ***]	Не обязательно	Поле заполняется в свободной форме	[detection_tool: ПО Kaspersky]
Дата и время выявления	[detect_time: ***]	❗ 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	[detect_time: 2020-11-18T12:34:02+07]
Дата и время завершения	[end_time: ***]	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	[end_time: 2020-11-19T11:50:02+07]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
Ограничительный маркер TLP	[tlp: ***]	❗ Обязательно	• TLP:WHITE • TLP:RED • TLP:GREEN • TLP:AMBER	[tlp: TLP:WHITE]
Заявитель	[reporter_name: ***]	❗ Обязательно	Поле заполняется в свободной форме согласно общепринятым правилам	[reporter_name: АО «Ромашка»]
Влияние на конфиденциальность	[confidentiality_impact: ***]	Не обязательно	• Высокое • Низкое • Отсутствует	[confidentiality_impact: Низкое]
Влияние на целостность	[integrity_impact: ***]	Не обязательно	• Высокое • Низкое • Отсутствует	[integrity_impact: Высокое]
Влияние на доступность	[availability_impact: ***]	Не обязательно	• Высокое • Низкое • Отсутствует	[availability_impact: Высокое]
Краткое описание иной формы последствий компьютерного инцидента	[custom_impact: ***]	Не обязательно	Поле заполняется в свободной форме	[custom_impact: Отсутствуют]
Утечка ПДн	[rkn_leak_pd: ***]	Не обязательно	Boolean: • true • false	• [rkn_leak_pd: true]
Общие сведения о контролируемом ресурсе				
Наименование	[affected_system_name: ***]	❗ Обязательно	Поле заполняется в свободной форме	[affected_system_name: АСУ "Управление распределением энергии"]
Информация о категорировании ОКИИ	[affected_system_category: ***]	❗ Обязательно	• Информационный ресурс не является объектом КИИ • Объект КИИ без категории значимости	[affected_system_category: Объект КИИ третьей категории значимости]

Наименование поля	Тег поля	Обязательность заполнения поля		Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
				• Объект КИИ третьей категории значимости • Объект КИИ второй категории значимости • Объект КИИ первой категории значимости	
Сфера функционирования	[affected_system_function: ***]	❗	Обязательно	• Здравоохранение • Наука • Транспорт • Связь • 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	[affected_system_function: Топливно-энергетический комплекс]
Наличие подключения к сети Интернет	[affected_system_connection: ***]	❗	Обязательно	Boolean: • true • false	[affected_system_connection: true]
Местоположение контролируемого ресурса					
Локация	[location: ***]	❗	Обязательно	В поле необходимо указать геокод основной единицы первого или первого и	[location: RU-NVS]

Наименование поля	Тег поля	Обязательность заполнения поля		Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
				второго уровня административно-территориального деления территории всех стран согласно стандарта ISO-3166-2 (https://www.iso.org/standard/72483.html) Например, для Новосибирской области согласно ISO-3166-2 установлен код " RU-NVS"	
Населенный пункт или геокоординаты	[city: ***]	Не обязательно		Поле заполняется в свободной форме	[city: Новосибирск]
Сведения об утечке персональных данных					
ИНН	[rkn_inn: ***]	❗	Обязательно, если заполнено поле Утечка ПДн	Поле заполняется только в виде цифр	[rkn_inn: 1111111111]
Наименование оператора	[rkn_full_name: ***]	❗	Обязательно, если заполнено поле Утечка ПДн	Поле заполняется в соответствии с регистрацией в ФНС.	[rkn_full_name: Акционерное общество «Ромашка»]
Адрес оператора	[rkn_address: ***]	❗	Обязательно, если заполнено поле Утечка ПДн	Адрес заполняется в формате: Индекс, Регион, Населенный пункт, Улица, Дом	[rkn_address: 111111, Московская область, г. Мытищи, ул. Примерная, д. 5]
Адрес электронной почты для отправки информации об уведомлении	[rkn_email: ***]	❗	Обязательно, если заполнено поле Утечка ПДн	Заполняется согласно общепринятым правилам написания Email-адресов.	[rkn_email: mail@mail.ru]
Предполагаемые причины, повлекшие	[rkn_reasons: ***]	❗	Обязательно, если заполнено	Поле заполняется в свободной форме	[rkn_reasons: Хакерская атака на сайт]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
нарушение прав субъектов ПД		поле Утечка ПДн		
Характеристики персональных данных	[rkn_pers_data: ***]	Обязательно, если заполнено поле Утечка ПДн	Поле заполняется в свободной форме	[rkn_pers_data: Клиенты магазина. В содержащихся записях были указаны номера телефонов, адреса электронной почты, адреса доставки и имена.]
Предполагаемый вред, нанесенный правам субъектов ПД	[rkn_damage: ***]	Обязательно, если заполнено поле Утечка ПДн	Поле заполняется в свободной форме	[rkn_damage: Низкий]
Принятые меры по устранению последствий инцидента	[rkn_measures: ***]	Не обязательно	Поле заполняется в свободной форме	[rkn_measures: После выявления инцидента были приняты меры по устранению ВПО.]
Дополнительный сведения	[rkn_add_info: ***]	Не обязательно	Поле заполняется в свободной форме	[rkn_add_info: Отсутствуют]
Информация о результатах внутреннего расследования инцидента	[rkn_investigation: ***]	Не обязательно	Поле заполняется в свободной форме	[rkn_investigation: Хакерская атака на сайт компании, повлекшая за собой распространение данных пользователей.]
Технические сведения об атакованном ресурсе				
IPv4-адрес	[related_observables_ipv4: [{"value":"***"}]]	Не обязательно	Заполняется в в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Это поле типа объект, у него может иметь несколько значений, например, {"value":"5.5.5.5"}, {"value":"2.2.2.2"} и т.д.	[related_observables_ipv4: [{"value":"5.5.5.5"}]]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
IPv6-адрес	[related_observables_ipv6: [{"value":"***"}]]	Не обязательно	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 (::). Это поле типа объект, у него может быть несколько значений, например, {"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6"}, {"value":"5050:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6"} и т.д.	[related_observables_ipv6: [{"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6"}]]
Доменное имя	[related_observables_domain: [{"value":"***"}]]	Не обязательно	Заполняется согласно общепринятым правилам написания доменных имен. У поля может быть несколько значений, например, {"value":"rmsh.ru"}, {"value":"lk.rmsh.ru"} и т.д.	[related_observables_domain: [{"value":"rmsh.ru"}]]
URI-адрес	[related_observables_uri: [{"value":"***"}]]	Не обязательно	Заполняется согласно общепринятым правилам написания URI-адресов. У поля может быть несколько значений, например, {"value":" urn:isbn:1234567890"}, {"value":" urn:isbn:0987654321"} и т.д.	[related_observables_uri: [{"value":"urn:isbn:1234567890"}]]
Email-адрес атакованного ресурса	[related_observables_email: [{"value":"***"}]]	Не обязательно	Заполняется согласно общепринятым правилам написания Email-адресов. У поля может быть несколько значений, например, {"value":" office@rmsh.ru"}, {"value":"info@rmsh.ru"} и т.д.	[related_observables_email: [{"value":"office@rmsh.ru"}]]
Сетевая служба и порт/протокол	[related_observables_service: [{"name":"***", "value":"***"}]]	Не обязательно	Поле типа объект, в которое записываются два значения: сетевая служба в ключ “name” и порт/протокол в ключ “value”.	[related_observables_service: [{"name":"Служба ошибок Windows", "value":"443/TCP"}]]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
			У поля может быть несколько значений, например, {"name":"Служба ошибок Windows", "value":"443/TCP"}, {"name":"Служба SSH", "value":"22/SSH"} и т.д.	
AS-Path до атакованной Автономной системы (ASN)	[related_observables_as_path: ***]	Не обязательно	Заполняется согласно общепринятым правилам написания AS-Path	[related_observables_as_path: 29225 198705]
Технические сведения о вредоносной системе				
IPv4-адрес вредоносной системы	[related_indicators_ipv4: [{"value":"***", "function":"***"}]]	Не обязательно	Заполняется в формате xxx.xxx.xxx.xxx, где 0<=xxx<=255, где каждая буква x представляет десятичную цифру. Незначащие нули можно не указывать. Для событий ИБ, связанных с ВПО, в теге "function" необходимо указать одно из следующих значений: • Центр управления ВПО; • Элемент инфраструктуры ВПО; • Источник распространения ВПО; • Тип не определен. Для событий ИБ, не связанных с ВПО, в теге "function" необходимо указать "Тип не определен". Это поле типа объект, у него может быть несколько значений, например, {"value":"2.2.2.2", "function":"Элемент инфраструктуры ВПО"}, {"value":"7.7.7.7", "function":"Тип не определен"} и т.д.	[related_indicators_ipv4: [{"value":"2.2.2.2", "function":"Элемент инфраструктуры ВПО"}, {"value":"7.7.7.7", "function":"Тип не определен"}]]
IPv6-адрес вредоносной системы	[related_indicators_ipv6: [{"value":"***", "function":"***"}]]	Не обязательно	Заполняется как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это	[related_indicators_ipv6: [{"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6"}]]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
			шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (::). Для событий ИБ, связанных с ВПО, в теге "function" необходимо указать одно из следующих значений: • Центр управления ВПО; • Элемент инфраструктуры ВПО; • Источник распространения ВПО; • Тип не определен. Для событий ИБ, не связанных с ВПО, в теге "function" необходимо указать "Тип не определен". Это поле типа объект, у него может быть несколько значений, например, {"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6", "function":"Элемент инфраструктуры ВПО"}, {"value":"5050:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6", "function":"Тип не определен"} и т.д.	
Доменное имя вредоносной системы	[related_indicators_domain: [{"value":"***", "function":"***"}]]	Не обязательно	Для событий ИБ, связанных с ВПО, в теге "function" необходимо указать одно из следующих значений: • Центр управления ВПО; • Элемент инфраструктуры ВПО; • Источник распространения ВПО; • Тип не определен.	[related_indicators_domain: [{"value":"ra1qcw.ru", "function":"Источник распространения ВПО"}]]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
			Для событий ИБ, не связанных с ВПО, в теге "function" необходимо указать "Тип не определен". Заполняется согласно общепринятым правилам написания доменных имен. У поля может быть несколько значений, например, {"value":"ra1qcw.ru", "function":"Источник распространения ВПО"}, {"value":"ra2qcw.ru", "function":"Источник распространения ВПО"} и т.д.	
URI-адрес вредоносной системы	[related_indicators_uri: [{"value":"***", "function":"***"}]]	Не обязательно	Для событий ИБ, связанных с ВПО, в теге "function" необходимо указать одно из следующих значений: • Центр управления ВПО; • Элемент инфраструктуры ВПО; • Источник распространения ВПО; • Тип не определен. Для событий ИБ, не связанных с ВПО, в теге "function" необходимо указать "Тип не определен". Заполняется согласно общепринятым правилам написания URI-адресов. У поля может быть несколько значений, например, {"value":" urn:isbn:1234567890", "function":"Источник распространения ВПО"}, {"value":" urn:isbn:0987654321", "function":"Источник распространения ВПО"} и т.д.	[related_indicators_uri: [{"value":"urn:isbn:0-486-27557-4", "function":"Источник распространения ВПО"}]]
Email-адрес вредоносного объекта	[related_indicators_email: [{"value":"***"}]]	Не обязательно	Заполняется согласно общепринятым правилам написания Email-адресов.	[related_indicators_email: [{"value":"jslee.jcr@gmail.com"}]]

Наименование поля	Тег поля	Обязательность заполнения поля	Справочник значений для заполнения поля (при заполнении необходимо выбрать одно из значений справочника) или требования к формату данных	Пример заполнения
			У поля может быть несколько значений, например, {"value":"jslee.jcr@gmail.com"}, {"value":"dark@mail.ru"} и т.д.	
Хеш-сумма вредоносного модуля	[malware_hash: [{"value":"***"}]]	Не обязательно	В поле указывается один из следующих форматов контрольной суммы: • sha256; • sha1; • md5. У поля может быть несколько значений, например, {"value":" ef537f25c895bfa 782526529a9b63d97aa631564d5 d789c2b765448c8635fb6c"}, {"value":" ef537f25c895bfa782233229a9b63 d97aa631564d5d789c2b765448c 8635fb6c"} и т.д.	[malware_hash: [{"value":"ef537f25c895bfa 782526529a9b63d97aa63 1564d5d789c2b765448 c8635fb6c"}]]
Описание используемых уязвимостей	[related_indicators_vuln: [{"value":"***"}]]	Не обязательно	Поле заполняется в свободной форме. У поля может быть несколько значений	[related_indicators_vuln: [{"value":"APT-группировка BlackEnergy использует целевые фишинговые письма, содержащие вредоносные документы Excel с макросами для заражения компьютеров в целевой сети."}]]
Номер подставной Автономной системы (ASN)	[related_indicators_asn: ***]	Не обязательно	Заполняется согласно общепринятым правилам написания номера ASN	[related_indicators_as: AS48666]
Наименование AS	[related_indicators_as: ***]	Не обязательно	Поле заполняется в свободной форме	[relatedIndicatorsas: AS-MAROSNET Moscow, Russia, RU]
Наименование LIR	[related_indicators_lir: ***]	Не обязательно	Поле заполняется в свободной форме	[related_indicators_lir: MAROSNET Telecommunication Company Network]

Ниже приведен пример Уведомления по ЭП с заполненными полями для типа события ИБ Заражение ВПО:

Общие сведения

Наименование организации владельца информационного ресурса [company_name: АО "Ромашка"]
Категория [category: Уведомление о компьютерном инциденте]
Тип события ИБ [type: Заражение ВПО]
Статус реагирования [activity_status: Проводятся мероприятия по реагированию]
Необходимость привлечения сил ГосСОПКА [assistance: true]
Краткое описание события ИБ [event_description: На хосте выявлен вирус BlackEnergy]
Сведения о средстве или способе выявления [detection_tool: ПО Kaspersky]
Дата и время выявления [detect_time: 2020-11-18T12:34:02+07]
Дата и время завершения [end_time: 2020-11-19T11:50:02+07]
Ограничительный маркер TLP [tlp: TLP:WHITE]
Заявитель [reporter_name: АО "Ромашка"]
Влияние на конфиденциальность [confidentiality_impact: Низкое]
Влияние на целостность [integrity_impact: Высокое]
Влияние на доступность [availability_impact: Высокое]
Краткое описание иной формы последствий компьютерного инцидента [custom_impact: Отсутствуют]
Утечка ПДн [rkn_leak_pd: true]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: АСУ "Управление распределением энергии"]
Информация о категорировании ОКИИ [affected_system_category: Объект КИИ третьей категории значимости]
Сфера функционирования [affected_system_function: Топливно-энергетический комплекс]
Наличие подключения к сети Интернет [affected_system_connection: true]

Местоположение контролируемого ресурса

Локация [location: RU-NVS]
Населенный пункт или геокоординаты [city: Новосибирск]

Сведения об утечке персональных данных

ИНН [rkn_inn: 1111111111]
Полное наименование [rkn_full_name: Акционерное общество «Ромашка»]
Адрес оператора [rkn_address: 111111, Московская область, г. Мытищи, ул. Примерная, д. 5]
Адрес электронной почты для отправки информации об уведомлении [rkn_email: mail@mail.ru]
Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: Хакерская атака на сайт]
Характеристики персональных данных [rkn_pers_data: Клиенты магазина. В содержащихся записях были указаны номера телефонов, адреса электронной почты, адреса доставки и имена]
Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: Низкий]
Принятые меры по устранению последствий инцидента [rkn_measures: После выявления инцидента были приняты меры по устранению ВПО]
Дополнительный сведения [rkn_add_info: Отсутствуют]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: Хакерская атака на сайт компании, повлекшая за собой распространение данных пользователей]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"5.5.5.5"}]]
IPv6-адрес [related_observables_ipv6: [{"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6"}]]
Доменное имя [related_observables_domain: [{"value":"rmsh.ru"}]]
URI-адрес [related_observables_uri: [{"value":"urn:isbn:1234567890"}]]
Email-адрес атакованного ресурса [related_observables_email: [{"value":"office@rmsh.ru"}]]
Сетевая служба и порт/протокол [related_observables_service: [{"name":"Служба ошибок Windows", "value":"443/TCP"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"2.2.2.2", "function":"Элемент инфраструктуры ВПО"}, {"value":"7.7.7.7", "function":"Тип не определен"}]]
IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"9090:5ffd:695e:fec4:8ecf:8bd0:e2d9:37e6", "function":"Источник распространения ВПО"}]]
Доменное имя вредоносной системы [related_indicators_domain: [{"value":"ra1qcw.ru", "function":"Источник распространения ВПО"}]]
URI-адрес вредоносной системы [related_indicators_uri: [{"value":"urn:isbn:0-486-27557-4", "function":"Источник распространения ВПО"}]]
Email-адрес вредоносного объекта [related_indicators_email: [{"value":"jslee.jcr@gmail.com"}]]
Хеш-сумма вредоносного модуля [malware_hash: [{"value":"ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c"}]]
Описание используемых уязвимостей [related_indicators_vuln: [{"value":"APT-группировка BlackEnergy использует целевые фишинговые письма, содержащие вредоносные документы Excel с макросами для заражения компьютеров в целевой сети"}]]

4. Шаблоны Уведомлений по ЭП

4.1. Шаблоны Уведомлений о компьютерном инциденте

4.1.1. Шаблон Использование контролируемого ресурса для проведения атак

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]
Категория [category: Уведомление о компьютерном инциденте]
Тип события ИБ [type: Вовлечение контролируемого ресурса в инфраструктуру ВПО]
Статус реагирования [activity_status: ***]
Необходимость привлечения сил ГосСОПКА [assistance: ***]
Краткое описание события ИБ [event_description: ***]
Сведения о средстве или способе выявления [detection_tool: ***]
Дата и время выявления [detect_time: ***]
Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

4.1.2. Шаблон Замедление работы ресурса в результате DDoS-атаки

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Замедление работы ресурса в результате DDoS-атаки]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.3. Шаблон Заражение ВПО

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Заражение ВПО]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Утечка ПДн [rkn_leak_pd: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Сведения об утечке персональных данных

ИНН [rkn_inn: ***]

Наименование оператора [rkn_full_name: ***]

Адрес оператора [rkn_address: ***]

Адрес электронной почты для отправки информации об уведомлении [rkn_email: ***]

Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: ***]

Характеристики персональных данных [rkn_pers_data: ***]

Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: ***]

Принятые меры по устранению последствий инцидента [rkn_measures: ***]

Дополнительный сведения [rkn_add_info: ***]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]

Хеш-сумма вредоносного модуля [malware_hash: [{"value":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.4. Шаблон Захват сетевого трафика

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Захват сетевого трафика]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

AS-Path до атакованной Автономной системы (ASN) [related_observables_as_path: ***]

Технические сведения о вредоносной системе

Номер подставной Автономной системы (ASN) [related_indicators_as: ***]

Наименование AS [relatedIndicatorsas: ***]

Наименование LIR [related_indicators_lir: ***]

4.1.5. Шаблон Компрометация учетной записи

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Компрометация учетной записи]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Утечка ПДн [rkn_leak_pd: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Сведения об утечке персональных данных

ИНН [rkn_inn: ***]

Наименование оператора [rkn_full_name: ***]

Адрес оператора [rkn_address: ***]

Адрес электронной почты для отправки информации об уведомлении [rkn_email: ***]

Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: ***]

Характеристики персональных данных [rkn_pers_data: ***]

Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: ***]

Принятые меры по устранению последствий инцидента [rkn_measures: ***]

Дополнительный сведения [rkn_add_info: ***]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.6. Шаблон Несанкционированное изменение информации

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Несанкционированное изменение информации]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.7. Шаблон Несанкционированное разглашение информации

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Несанкционированное разглашение информации]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Утечка ПДн [rkn_leak_pd: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Сведения об утечке персональных данных

ИНН [rkn_inn: ***]

Наименование оператора [rkn_full_name: ***]

Адрес оператора [rkn_address: ***]

Адрес электронной почты для отправки информации об уведомлении [rkn_email: ***]

Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: ***]

Характеристики персональных данных [rkn_pers_data: ***]

Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: ***]

Принятые меры по устранению последствий инцидента [rkn_measures: ***]

Дополнительный сведения [rkn_add_info: ***]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]
IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]
Доменное имя [related_observables_domain: [{"value":"***"}]]
URI-адрес [related_observables_uri: [{"value":"***"}]]
Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]
Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]
IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]
Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]
URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]
Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]
Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.8. Шаблон Публикация на ресурсе запрещенной законодательством РФ информации

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]
Категория [category: Уведомление о компьютерном инциденте]
Тип события ИБ [type: Публикация на ресурсе запрещенной законодательством РФ информации]
Статус реагирования [activity_status: ***]
Необходимость привлечения сил ГосСОПКА [assistance: ***]
Краткое описание события ИБ [event_description: ***]
Сведения о средстве или способе выявления [detection_tool: ***]
Дата и время выявления [detect_time: ***]
Дата и время завершения [end_time: ***]
Ограничительный маркер TLP [tlp: ***]
Заявитель [reporter_name: ***]
Влияние на конфиденциальность [confidentiality_impact: ***]
Влияние на целостность [integrity_impact: ***]
Влияние на доступность [availability_impact: ***]
Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]
Информация о категорировании ОКИИ [affected_system_category: ***]
Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.9. Шаблон Успешная эксплуатация уязвимости

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Успешная эксплуатация уязвимости]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Утечка ПДн [rkn_leak_pd: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Сведения об утечке персональных данных

ИНН [rkn_inn: ***]

Наименование оператора [rkn_full_name: ***]

Адрес оператора [rkn_address: ***]

Адрес электронной почты для отправки информации об уведомлении [rkn_email: ***]

Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: ***]

Характеристики персональных данных [rkn_pers_data: ***]

Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: ***]

Принятые меры по устранению последствий инцидента [rkn_measures: ***]

Дополнительный сведения [rkn_add_info: ***]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.1.10. Шаблон Событие не связано с компьютерной атакой

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерном инциденте]

Тип события ИБ [type: Событие не связано с компьютерной атакой]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Влияние на конфиденциальность [confidentiality_impact: ***]

Влияние на целостность [integrity_impact: ***]

Влияние на доступность [availability_impact: ***]

Краткое описание иной формы последствий компьютерного инцидента [custom_impact: ***]

Утечка ПДн [rkn_leak_pd: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Сведения об утечке персональных данных

ИНН [rkn_inn: ***]

Наименование оператора [rkn_full_name: ***]

Адрес оператора [rkn_address: ***]

Адрес электронной почты для отправки информации об уведомлении [rkn_email: ***]

Предполагаемые причины, повлекшие нарушение прав субъектов ПД [rkn_reasons: ***]

Характеристики персональных данных [rkn_pers_data: ***]

Предполагаемый вред, нанесенный правам субъектов ПД [rkn_damage: ***]

Принятые меры по устранению последствий инцидента [rkn_measures: ***]

Дополнительный сведения [rkn_add_info: ***]

Информация о результатах внутреннего расследования инцидента [rkn_investigation: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

4.2. Шаблоны Уведомлений о компьютерной атаке

4.2.1. Шаблон DDoS-атака

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: DDoS-атака]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.2. Шаблон Неудачные попытки авторизации

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Неудачные попытки авторизации]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.3. Шаблон Попытки внедрения ВПО

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Попытки внедрения ВПО]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]

Хеш-сумма вредоносного модуля [malware_hash: [{"value":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.4. Шаблон Попытки эксплуатации уязвимости

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Попытки эксплуатации уязвимости]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.5. Шаблон Публикация мошеннической информации

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Публикация мошеннической информации]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

URI-адрес [related_observables_uri: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.6. Шаблон Сетевое сканирование

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Сетевое сканирование]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]

4.2.7. Шаблон Социальная инженерия

Общие сведения

Наименование организации владельца информационного ресурса [company_name: ***]

Категория [category: Уведомление о компьютерной атаке]

Тип события ИБ [type: Социальная инженерия]

Статус реагирования [activity_status: ***]

Необходимость привлечения сил ГосСОПКА [assistance: ***]

Краткое описание события ИБ [event_description: ***]

Сведения о средстве или способе выявления [detection_tool: ***]

Дата и время выявления [detect_time: ***]

Дата и время завершения [end_time: ***]

Ограничительный маркер TLP [tlp: ***]

Заявитель [reporter_name: ***]

Общие сведения о контролируемом ресурсе

Наименование [affected_system_name: ***]

Информация о категорировании ОКИИ [affected_system_category: ***]

Сфера функционирования [affected_system_function: ***]

Наличие подключения к сети Интернет [affected_system_connection: ***]

Местоположение контролируемого ресурса

Локация [location: ***]

Населенный пункт или геокоординаты [city: ***]

Технические сведения об атакованном ресурсе

IPv4-адрес [related_observables_ipv4: [{"value":"***"}]]

IPv6-адрес [related_observables_ipv6: [{"value":"***"}]]

Доменное имя [related_observables_domain: [{"value":"***"}]]

Email-адрес атакованного ресурса [related_observables_email: [{"value":"***"}]]

Сетевая служба и порт/протокол [related_observables_service: [{"name":"***", "value":"***"}]]

Технические сведения о вредоносной системе

IPv4-адрес вредоносной системы [related_indicators_ipv4: [{"value":"***", "function":"***"}]]

IPv6-адрес вредоносной системы [related_indicators_ipv6: [{"value":"***", "function":"***"}]]

Доменное имя вредоносной системы [related_indicators_domain: [{"value":"***", "function":"***"}]]

URI-адрес вредоносной системы [related_indicators_uri: [{"value":"***", "function":"***"}]]

Email-адрес вредоносного объекта [related_indicators_email: [{"value":"***"}]]

Описание используемых уязвимостей [related_indicators_vuln: [{"value":"***"}]]