Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России

(Версия 2.3)

1. Общие положения

1.1. Настоящий Регламент определяет формат и сроки предоставления информации участником информационного взаимодействия в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления Банка России (далее – ФинЦЕРТ) (приложение к настоящему Регламенту).

1.2. Настоящий регламент служит для апробации выбранных форматов передачи данных и внесения соответствующих изменений по результатам апробации.

1.3. Предложения по оптимизации выбранного формата передачи данных необходимо направлять на адрес электронной почты info_fincert@cbr.ru с темой сообщения *[оптимизация формата передачи]*.

2. Порядок передачи информации Участником информационного взаимодействия

2.1. Передача информации, приведённой в приложении к настоящему Регламенту, осуществляется с использованием электронной почты на адрес fincert@cbr.ru.

2.2. По желанию передающей стороной данные могут передаваться в архиве с паролем, при этом пароль должен быть доведен до работников ФинЦЕРТ с использованием альтернативных каналов связи. Требования к сложности пароля определяются передающей стороной.

2.3. В случае передачи на исследование образцов вредоносного программного обеспечения (вирусов), образцы передаются в ФинЦЕРТ в архиве (**rar** или **zip)** с паролем, при этом пароль должен быть одним из следующих: **virus** или **infected**. В случае, если в передаваемом архиве не установлен пароль, то он удаляется автоматически.

Перечень информации, предоставляемой участником информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России

1. Основные обозначения

КАРТОЧКА - Код (INT)
Направлен на инфраструктуру организации (внутренний)

Код (MLW)
- Выявление вредоносного ПО (в т.ч. целевая атака (APT)). Учитываются атаки на любые устройства инфраструктуры (в том числе банкоматы, электронные и платёжные терминалы) при выполнении хотя бы одного из условий:
- Выявление вредоносного кода, не определяемого антивирусным ПО или определяемого не более 5 антивирусами на Virus Total;
- Обнаружение на объекте информационной инфраструктуры антивирусным ПО или иными СЗИ вредоносного ПО или подозрительного ПО, направленного на этот объект информационной инфраструктуры, согласно вердикту антивирусного ПО или иного СЗИ;
- Обнаружение на объекте информационной инфраструктуры подозрительных файлов (процессов), в т.ч. неисполняемых, недетектируемых антивирусным ПО или хостовыми системами обнаружения вторжений (HIPS).

Код (DOS)
- Выявление DoS/DDoS, сбоев в работе оборудования и каналов связи, вызванных внешними причинами

Код (BAN)
- Физическое и/или логическое воздействие на объекты информационной инфраструктуры.

Физическое воздействие – установка скиммингового оборудования, несанкционированный доступ к интерфейсам управления (в т.ч. банкоматов и терминалов), повреждение оборудования с целью установки сторонних аппаратных устройств или хищения находящихся в устройстве денежных средств.
Логическое воздействие – внедрение стороннего программного обеспечения либо модификация существующих настроек системного программного обеспечения.

Код (URL)
- Выявление ресурсов в информационно-телекоммуникационной сети Интернет, связанных с финансовой сферой (в т.ч. приобретение товаров или услуг), содержащих противоправный контент либо недостоверную информацию, в частности фишинговой направленности. К данному

виду инцидентов также относятся ресурсы, предназначенные для распространения вредоносного кода, включая ресурсы, используемые для рассылки мошеннических электронных писем, а также центры управления бот-сетями.
В рассматриваемые инциденты могут быть включены сведения о ресурсах соответствующей направленности, выявленных клиентами организации. Также могут быть включены обнаруженные ссылки на скачивание ВК либо ссылки, определяемые как подозрительные/вредоносные антивирусным ПО / иным СЗИ.

Код (SOI)

- Выявление телефонных номеров и почтовых электронных писем, используемых для распространения недостоверной информации, вредоносного содержимого и (или) побуждения работника организации к совершению несанкционированных действий путем обмана или злоупотребления доверием (включая письма, содержащие угрозы в адрес организации).

Код (EXP)

- Выявление попыток эксплуатации уязвимостей. К эксплуатации уязвимостей относится, например, использование SQL инъекций. Кроме того, к эксплуатации уязвимостей относятся действия внутреннего нарушителя. Попытки эксплуатации могут быть выявлены как средствами IDS / IPS / HIPS, так и специалистами организации либо в результате обращения гражданина в организацию о возможной попытке эксплуатации уязвимости в отношении организации.

Код (BRT)

- Выявление попыток взлома учетных записей (как внутри сети, так и на веб-ресурсах, принадлежащих организации) посредством автоматизированного подбора комбинаций паролей и логинов. Условия уведомления приведены в описании кода.

Код (SCN)

- Выявление попыток сканирования портов для взлома сети. Условия уведомления приведены в описании кода.

Код (OTH)

- Прочее.

КАРТОЧКА - Код (EXT)

Направлен на клиента организации (внешний).

Код (MLW) - Совершение несанкционированного перевода денежных средств в результате воздействия вредоносного ПО.

Код (SOI) - Совершение несанкционированного перевода денежных средств в результате обмана или злоупотребления доверием.

Код (SIM) - Совершение несанкционированного перевода денежных средств в результате изменения IMSI SIM-карты, смена IMEI телефона.

Код (P2P) - Совершение несанкционированного перевода денежных средств в результате использования фишингового ресурса.

Код (LST) - Совершение несанкционированного перевода денежных средств в результате утраты электронного средства платежа.

Код (OTH) - Совершение несанкционированного перевода денежных средств в результате иных причин.

КАРТОЧКА – Код PUB

Информация о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая размещение информации на официальных сайтах в информационно-телекоммуникационной сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций.

2. Информация об инциденте (Электронная форма Инцидента)

Наименование поля	**Описание**		
	Описание поля	**Формат данных**	**Пример**
Служебные свойства инцидента			
Тип документа	Служебное поле Описывает тип документа	Только "incident"	incident
Версия документа	Служебное поле Описывает версию документа	X.Y	1.0
Количество правок (редакций) документа	Служебное поле Описывает количество правок (редакций) документа	int32	4
Хэш файла	Служебное поле Хэш md5 всего содержимого документа (за исключением поля hash), служит для индикации случайного повреждения документа	md5 hash	0ba8927585c7824320ad959f8eb4dc6e

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Базовые свойства инцидента			
Идентификатор инцидента со стороны участника	Идентификатор инцидента. Участником генерируется в формате yyyyMMddHHmmss (yyyy = год, MM = месяц, dd = день, hh = часы, mm = минуты, ss = секунды)'	yyyyMMddHHmmss	"20170901112233"
Дата и время публикации инцидента	дата и время публикации инцидента	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Дата и время последнего изменения инцидента	Дата и время последнего изменения инцидента	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Дата и время фиксации КИ	Дата и время фиксации КИ	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Идентификатор организации	Идентификатор организации (уникальный номер организации, напр. номер лицензии Банка России)	int32	4
Тип организации	Тип организации Значение из списка	• 1 #=КО • 2 #=НКО • 3 #=МФО • 4 #=Страховая организация • 5 #=Вендор ИБ • 6 #=Иные государственные организации • 7 #=Иные коммерческие организации • 8 #=Иностранные организации • 9 #=CERTы (в т.ч. иностранные) - для возможности организации адресных рассылок	4

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Описание инцидента	Описание инцидента	string	"Инцидент был обнаружен при … и т.д."
Место происшествия инцидента	Место происшествия инцидента		
Субъект федерации	Код ОКАТО верхнего уровня (2 цифры - обязательно)	Код ОКАТО верхнего уровня из 2-х цифр	"10"
Название населенного пункта	Название населенного пункта	String	"Москва"
Принятые меры	Меры, принятые участником для ликвидации последствий инцидента	string	"В рамках инцидента было сделано .."
Ущерб в результате инцидента.	Ущерб в результате инцидента. Пустое поле означает отсутствие ущерба	string	"Потеряны важные данные"
Показывает, нужна ли консультация/помощь FinCERT	Показывает, нужна ли консультация/помощь FinCERT	• HLP • NND	HLP
Основной верхнеуровневый код инцидента	Основной верхнеуровневый код инцидента (куда направлен): на инфраструктуру организации/в организации или на клиента/у клиента	• EXT • INT	EXT

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Код конкретного типа инцидента	Код конкретного типа инцидента	# Общие для векторов EXT и INT • MLW • SOI • OTH # Специфичный для вектора INT • DOS • BAN • EXP • BRF • SPM • BCC • PHI • MLR # Специфичный для вектора EXT • SIM • P2P • LST	DOS
Вложения к инциденту	Заполняется следующими данными: • комментарий к вложению; • файл (имя файла + размер файла в байтах — если размер меньше 5 МБ + base64 файла); • url адрес для скачивания файла (если размер больше 5 МБ), с использованием протоколов FTP, HTTP, HTTPS		

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Примечание к вложению	Примечание к вложению	string	В этом файле/архиве находятся логи
Время когда файл был прикреплен	Время, когда файл был прикреплен	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Информация о прикрепленном файле	Информация о прикрепленном файле		
Имя файла	Имя файла	string	
Размер файла в байтах	Размер файла в байтах	string	
Файл в формате base64	Файл в формате base64	string	
Ссылка на файл	Внешняя ссылка на скачивание (если размер файла больше 5 МБ)	string	http://drive.google.com/asdasdasd
Вектор инцидента (vectors)			
EXT (Направлен на клиента организации)			
Способ осуществления несанкционированной операции	Способ осуществления несанкционированной операции	• SMS # SMS банкинг • MBB # Приложение для мобильного банкинга • BRW # Интернет-банкинг • PCW # Система «Банк-клиент» • ATM # Банкомат • POS # POS терминал • SST # Платежный терминал • CNP # E-commerce. Платежи в сети интернет без предъявления карты	POS
Способ перевода	Способ перевода		
Тип способа перевода	Тип способа перевода	• ACC # Перевод по номеру счета	ACC

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
		• PLC # Перевод по номеру карты • OTH # Иное	
Примечание к выбранному значению	Примечание к выбранному значению	string	""
Трансграничность	Трансграничность	• CRB # Трансграничный перевод • DOM # Внутри страны	CRB
Дополнительное подтверждение транзакции	Дополнительное подтверждение транзакции	• 3DS # Транзакция подтверждена с использованием 3D Secure • OAA # Иной способ подтверждения • NAA # Транзакция без подтверждения	OAA
Информация об обращении в правоохранительные органы	Информация об обращении в правоохранительные органы	• POL # Обращение есть • NPL # Обращения нет • UNK # Клиент не предоставил информацию	UNK
INT (Направлен на инфраструктуру организации)			
Сработавшие сигнатуры	Список сработавших сигнатур		
Идентификатор сигнатуры	Идентификатор сигнатуры	string	Sid 1-1298
Средство обнаружения	Средство обнаружения	string	
Источник получения сигнатуры	Источник получения сигнатуры	string	
Количество сработок сигнатуры	Количество сработок сигнатуры	int32	
Влияние инцидентов (impacts)			
MLW (Вредоностное программное обеспечение)			

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Внешний IP-адрес ЭВМ	Указывается IP-адрес, с которым зараженная ЭВМ получает доступ в интернет	IPv4	
Выявленные взаимодействия с ЦУ или другими ресурсами	Заполняется в случае выявления взаимодействия зараженной ЭВМ с каким-либо доменным именем или IP-адресом, которые могут являться ЦУ или другим вредоносным ресурсом. Возможные значения: • доменное имя; • IP-адрес; • URL Поле может содержать несколько значений		
Доменное имя	Доменное имя	domain	
IP-адрес	IP-адрес	IPv4	
URL	URL	URL	
Классификаторы	Заполняется по мере поступления информации и содержит тип выявленного ВПО по классификации какого-либо АВС: • наименование АВС; • тип ВПО Поле может содержать несколько значений		
Наименование АВС	Наименование антивирусной системы	string	Касперский
Классификатор	Как ВПО классифицирует указанная антивирусная система	string	Вирус

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Образцы ВПО	Коллекция Образцов ВПО. Один образец может характеризоваться: • или хэшем • или прикрепленным вложением		
Контрольная сумма выявленного образца ВПО	Заполняется контрольными суммами выявленного образца ВПО. Для каждого образца ВПО должна быть своя хеш-сумма		
Контрольная сумма в формате MD5	Контрольная сумма в формате MD5	string	
Контрольная сумма в формате SHA-1	Контрольная сумма в формате SHA-1	string	
Контрольная сумма в формате SHA-256	Контрольная сумма в формате SHA-256	string	
Файл ВПО	Заполняется в случае передачи вместе с ККИ файла, выявленного ВПО. Образец выявленного ВПО должен быть заархивирован в формате RAR с использованием пароля “infected”. Размер файла не должен превышать 5 МБ	Формат из секции attachments базовых полей инцидента	
Адреса электронных почтовых ящиков, с которых поступило письмо с вложением	Заполняется в случае, если ВПО было прислано на электронный почтовый ящик ведомства. В поле также должен быть указан IP-адрес последнего почтового сервера, через который было передано письмо. Поле может содержать несколько значений		

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Адрес электронного почтового ящика отправителя	Адрес электронного почтового ящика отправителя	email	
IP-адрес последнего почтового сервера	IP-адрес последнего почтового сервера	IPv4	
Имя файла с исходным кодом электронного письма	Заполняется в случае, если ВПО было прислано на электронный почтовый ящик ведомства. Указываются имя и размер прикрепленного файла	Формат из секции attachments базовых полей инцидента	
Адрес вредоносного ресурса, с которого было загружено ВПО	Заполняется в случае, если ВПО было скачано по ссылке, присланной на электронный почтовый ящик ведомства. Возможные значения: • доменное имя; • IP-адрес; • URL (также URL ресурса, с которого пользователь лично скачал ВПО)	string	
Доменное имя	Доменное имя	string	
IP-адрес	IP-адрес	string	
URL	URL	string	
Выявленные индикаторы компрометации	В случае, если участник обладает какими-то индикаторами компрометации (IOC), их можно указать		
Сетевые индикаторы	Сетевые индикаторы		
Обращение по IP-адресу/URL	Обращение по IP-адресу/URL	string	
Модификация текущих сетевых настроек	Модификация текущих сетевых настроек	string	

Наименование поля	Описание		
	Описание поля	Формат данных	Пример
Сокрытие следов сетевого взаимодействия	Сокрытие следов сетевого взаимодействия (удаление маршрутов, записей журналов сетевых устройств и т.д.)	string	
Файловые индикаторы	Файловые индикаторы		
Создание	Создание	string	
Изменение	Изменение	string	
Удаление файлов	Удаление файлов	string	
Индикаторы реестра ОС Windows	Индикаторы реестра ОС Windows		
Создание	Создание	string	
Изменение	Изменение	string	
Удаление файлов	Удаление файлов	string	
Индикаторы, связанные с процессами	Индикаторы, связанные с процессами		
Запуск процесса	Запуск процесса	string	
Изменение запущенного процесса	Изменение запущенного процесса	string	
Завершение процесса	Завершение процесса	string	
Иные индикаторы	Иные индикаторы	string	
Отчет средств динамического анализа кода в виде вложения	Отчет средств динамического анализа кода в виде вложения	Формат из секции attachments базовых полей инцидента	
Предполагаемый способ заражения	Предполагаемый способ заражения		
Тип предполагаемого способа заражения	Тип предполагаемого способа заражения	EML # По каналам электронной почты DSD # С носителя информации LCL # Распространение по локальной сети OTH # Иной способ	

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Примечание к выбранному типу	Примечание к выбранному типу	string	
SOI (социальная инженерия)			
Тип социальной инженерии	Тип социальной инженерии	• MOB # Звонок с мобильного телефонного номера • TPH # Звонок с телефонного номера 8-800 • SMS # СМС-сообщение • SNW # Социальная инженерия с использованием социальных сетей • MSG # Социальная инженерия с использованием средств мгновенных сообщений	
Дополнительное описание	Дополнительное описание	string	
Номер телефона в формате +7(XXX)XXXXXXX	В случае кодов (MOB) (TPH) – дополнительно в формате +7(XXX)XXXXXXX указать номер телефона. В случае кодов (SMS) (SNW) (MSG) указание номера отправителя.		
Вложение к секции	В случае кодов (SMS) (SNW) (MSG) дополнительно приложить фотографию (Файл) сообщения	Формат из секции attachments базовых полей инцидента	
OTH (другое)			
Другое	Другое		
Примечание	Примечание	string	

Наименование поля	Описание		
	Описание поля	Формат данных	Пример
DDOS / DOS (Отказ в обслуживании)			
Список описаний DOS атак			
Пострадавший ресурс	Пострадавший ресурс Заполняется любое из вложенных полей или их комбинация		
Адрес ресурса	Адрес ресурса	IPv4	
Назначение ресурса	Назначение ресурса	string	
Доменное имя	Доменное имя	domain	
URL	URL	url	
Тип сервиса	Тип сервиса (ssh, ftp и тд) в свободной форме	string	
Пострадавшая сеть	Пострадавшая сеть	string	
Источники атаки	Источники атаки, список IP адресов		
Адрес ресурса	Адрес ресурса	IPv4	
Тип атаки	Тип атаки		
Тип	Тип	• 1 # "L2/3: ICMP-flood" • 2 # "L2/3: NTP-amplification" • 3 # "L2/3: TFTP-amplification" • 4 # "L2/3: SENTINEL-amplification" • 5 # "L2/3: DNS-amplification" • 6 # "L2/3: SNMP-amplification" • 7 # "L2/3: SSDP-amplification" • 8 # "L2/3: CHARGEN-amplification" • 9 # "L2/3: RIPv1-amplification"	

Наименование поля	Описание		
	Описание поля	Формат данных	Пример
		• 10 # "L2/3: BitTorrent-amplification" • 11 # "L2/3: QTPD-amplification" • 12 # "L2/3: Quake-amplification" • 13 # "L2/3: LDAP-amplification" • 14 # "L2/3: 49ad34-amplification" • 15 # "L2/3: Portmap-amplification" • 16 # "L2/3: Kad-amplification" • 17 # "L2/3: NetBIOS-amplification" • 18 # "L2/3: Steam-amplification" • 19 # "L3: DPI-attack" • 20 # "L4: LAND-attack" • 21 # "L4: TCP-SYN-attack" • 22 # "L4: TCP-ACK-attack" • 23 # "L4: Smurf-attack" • 24 # "L4: ICMP/UDP-frag" • 25 # "L4: TCP-frag" • 26 # "L6: SSL-attack" • 27 # "L7: DNS Water Torture Attack"	

Наименование поля	Описание		
	Описание поля	Формат данных	Пример
		• 28 # "L7: Wordpress Pingback DDoS" • 29 # "L7: DNS-flood" • 30 # "L7: HTTP/S-flood" • 31 # "L7: FTP-flood" • 32 # "L7: SMTP-flood" • 33 # "L7: VoIP/SIP-attack" • 34 # "L7: POP3-flood" • 35 # "L7: SlowRate-attack" • 36 # "Другое"	
Примечание к выбранному типу	Примечание к выбранному типу	string	
Мощность атаки	Мощность атаки		
Количество пакетов в секунду	Количество пакетов в секунду	number	
Количество мегабит в секунду	Количество мегабит в секунду	number	
Количество запросов в секунду	Количество запросов в секунду	number	
Время начала	Время начала	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Время окончания	Время окончания	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
Негативное влияние	Негативное влияние		
Тип негативного влияния	Тип негативного влияния	NAW # Прерывание доступности ресурса OTH # Иные негативные последствия NCQ # Негативного влияния не было	NAW

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Примечание к выбранному типу	Примечание к выбранному типу	string	
BAN (Физическое воздействие на систему)			
Объект, подвергшийся воздействию	Объект, подвергшийся воздействию		
Тип объект, подвергшийся воздействию	Тип объект, подвергшийся воздействию	• ATM # Банкомат • CIN # Банкомат с возможностью приема наличных денежных средств • RES # Банкомат с функцией ресайклинга (recycling) • POS # POS-терминал • SST # Платежный терминал • OTH # Иной объект	
Примечание к выбранному значению	Примечание к выбранному значению	string	
Тип атаки	Тип атаки		
Тип	Тип	• BBX # Атаки «блэкбокс» • DSP # Атаки «прямой диспенс» и их разновидности • SKM # Скимминг • OTH # Иная атака	
Примечание к выбранному значению	Примечание к выбранному значению	string	
Вложение к секции		Формат из секции attachments базовых полей инцидента	
SIM (Атака с подменой номера)			

Наименование поля	Описание		
	Описание поля	Формат данных	Пример
Название оператора связи	Название оператора связи	string	
LST (Утрата электронного средства платежа)			
Дата направления информации об утрате ЭСП	Дата направления информации об утрате ЭСП	yyyyMMdd HH:mm:ss UTC+z	"20170901 11:22:33 UTC+3"
EXP (Эксплуатация уязвимости)			
Информация о пострадавшей ЭВМ	Информация о пострадавшей ЭВМ		
IP-адрес	IP-адрес	IPv4	
Доменное имя	Доменное имя	domain	
URL	URL	url	
Тип сервиса	Тип сервиса	string	
Источники атаки	Указывается IP-адрес, с которого была выявлена эксплуатация какой-либо уязвимости. Также URL ресурса, при заходе на который была поэксплуатирована уязвимость.		
IP-адрес	IP-адрес	IPv4	
Адрес ресурса	Адрес ресурса	url	
Идентификатор уязвимости	В случае выявления факта эксплуатации уязвимости неправильно настроенного сетевого сервиса необходимо указать его тип и описание уязвимости. Если выявлена уязвимость программного обеспечения, должен быть указан ее тип по классификации ФСТЭК, CVE, MS или другой	string	CVE-123123

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Метрика CVSS	Указать метрику CVSS v 3.0 (если определена) (указать максимально возможное количество метрик из перечисленных: базовая метрика, временная метрика, контекстная метрика, метрика окружения)	Формат CVSS	
Формирование CVSS вручную	Поля ниже заполняются только при отсутствии CVE ID / CVSS		
Вектор атаки	Вектор атаки	• NET # Сетевой • ASN # Соседняя сеть • LOC # Локальный • PHY # Физический	NET
Сложность эксплуатации	Сложность эксплуатации	• HGH # Высокий уровень сложности эксплуатации • LOW # Низкий уровень сложности эксплуатации • NON # Затрудняюсь определить	LOW
Требуемый уровень привилегий	Требуемый уровень привилегий	• ADM # Высокий (административный) уровень привилегий • USR # Низкий (пользовательский) уровень привилегий • NON # Аутентификация для эксплуатации не требуется	NON
Необходимость взаимодействия с пользователем	Необходимость взаимодействия с пользователем	• MAN # Действия требуются • AUT # Действия не требуются	MAN

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Влияние на конфиденциальность	Влияние на конфиденциальность	• NON # Отсутствует • MDL # Среднее • HGH # Высокое	MON
Влияние на целостность	Влияние на целостность	• NON # Отсутствует • MDL # Среднее • HGH # Высокое	MON
Влияние на доступность	Влияние на доступность	• NON # Отсутствует • MDL # Среднее • HGH # Высокое	MON
P2P (Фишинговый ресурс)			
URL ресурса	URL ресурса	url	
BRF (Подбор паролей)			
Адрес пострадавшей системы	Адрес пострадавшей системы		
IP-адрес	IP-адрес	IPv4	
URL	URL	url	
Тип Сервиса	Заполняется по мере поступления данных и содержит информацию о типе сетевого сервиса, на который была направлена атака	string	
Источники атаки	Источники атаки		
IP-адрес	IP-адрес	IPv4	
Информация о скомпрометированной учетной записи	Заполняется информацией о скомпрометированной учетной записи. Указываются учетная запись пользователя и ее полномочия		
Учетная запись	Учетная запись	string	iivanov
Привилегии	Привилегии	string	"Администратор"
SPM (Спам)			
Адресаты рассылки спама	Адресаты рассылки спама		
Адрес электронной почты	Адрес электронной почты	email	

Наименование поля	Описание		
	Описание поля	**Формат данных**	**Пример**
Источники рассылки	Доменное имя и IP-адрес ресурса, с которого рассылался спам		
IP-адрес	IP-адрес	IPv4	
Доменное имя	Доменное имя	domain	
PHI (Фишинг)			
Адрес легитимного ресурса	В данном поле указываются доменное имя и/или IP-адрес легитимного ресурса		
IP-адрес	IP-адрес	IPv4	
Доменное имя	Доменное имя	domain	
Адрес фишингового ресурса	Указываются URL и IP-адрес ресурса, на котором была размещена фишинговая информация		
IP-адрес	IP-адрес	IPv4	
URL	URL	url	
MLR (Вредоносный ресурс)			
Информация о пострадавшей системе	Указываются URL и IP-адрес, на которых был выявлен вредоносный ресурс		
IP-адрес	IP-адрес	IPv4	
URL	URL	url	
Описание вредоностной активности	Описание вредоностной активности	string	

3. Типовая форма описания угрозы (Электронная форма Угрозы)

<table>
<tr><th>Название поля</th><th>Описание поля (должно быть представлено в качестве подсказки при заполнении)</th><th>Пример</th></tr>
<tr><td>Наименование угрозы</td><td>Текстовое поле
Информация об угрозе, на основе которой возможно установить причину и (или) последствия угрозы. Наименование уязвимости должно быть представлено на русском языке (в скобках на английском языке – при необходимости)</td><td>Вредоносный код JS.Downloader</td></tr>
<tr><td>Идентификатор угрозы</td><td>Текстовое поле (присваивается автоматически разрабатываемой системой)
Представляет собой алфавитно-цифровой код, включающий код базы данных угроз (ФинЦЕРТ), код угрозы, год, месяц и дату выявления угрозы, и порядковый номер угрозы, выявленной за текущий день. При определении идентификатора угрозы код базы данных уязвимостей, код угрозы, дату выявления угрозы и ее порядковый номер должны быть отделены друг от друга знаком «-», при этом знак пробела не ставится.
<table>
<tr><th>Наименование угрозы</th><th>Код угрозы</th></tr>
<tr><td>Вредоносное программное обеспечение</td><td>ВК</td></tr>
<tr><td>Эксплуатация уязвимости</td><td>ЭУ</td></tr>
<tr><td>DDoS</td><td>ОО</td></tr>
<tr><td>ЦУ бот-сети</td><td>ЦУ</td></tr>
<tr><td>Фишинг</td><td>ФШ</td></tr>
<tr><td>Вредоносный ресурс</td><td>ВР</td></tr>
<tr><td>другое</td><td>ДР</td></tr>
</table></td><td>FinCERT-ВК-2016-1234</td></tr>
<tr><td>Краткое описание угрозы</td><td>Текстовое поле
Представляет собой текстовую информацию об угрозе и возможностях ее использования</td><td>Вредоносный код представляет собой загрузчик шифровальщика</td></tr>
<tr><td>Класс угрозы</td><td>Текстовое поле (выбор из закрытого списка)
– Вредоносное программное обеспечение
<table>
<tr><td rowspan="4">Индикаторы компрометации</td><td>Текстовые поля</td></tr>
<tr><td>В формате Yara (если есть)</td></tr>
<tr><td>В формате Open IOC (если есть)</td></tr>
<tr><td>В формате XML (если есть)</td></tr>
</table></td><td></td></tr>
</table>

	Иные форматы
Антивирусные решения, детектирующие ВПО	Текстовое поле

– Эксплуатация уязвимости

Идентификатор уязвимости	Текстовое поле с возможностью перехода на карточку уязвимости (Стандартизированный (CVE, ФСТЭК))
Описание методики эксплуатации	Текстовое поле с возможностью вставки изображений (Допускается ссылка на POC (proof of concept) уязвимости)

– DDoS

Атакующие IP адреса	Текстовое поле
Тип атаки	Текстовое поле
Прогнозируемое усиление (если есть)	Текстовое поле
Прогнозируемая мощность (если есть)	Текстовое поле

– ЦУ бот-сети

IP-адрес или доменное имя	Текстовое поле
Тип и общие сведения о бот-сети	Текстовое поле
Каким образом выявлен	Текстовое поле

– Фишинг

IP-адрес или доменное имя ресурса	Текстовое поле
Дата обнаружения ресурса	Дата
Технические заголовки письма (при наличии)	Текстовое поле
Текст письма (при наличии)	Текстовое поле

– Вредоносный ресурс

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>IP-адрес или доменное имя ресурса</td><td>Текстовое поле</td></tr>
<tr><td>Дата обнаружения ресурса</td><td>Дата</td></tr>
<tr><td>Причины, почему ресурс подозревается вредоносным</td><td>Текстовое поле</td></tr>
</table>
– Мошеннический телефонный номер
<table>
<tr><td>Дата и время звонка (смс)</td><td>Дата</td></tr>
<tr><td>Текст смс</td><td>Текстовое поле</td></tr>
<tr><td>Номер (сотовый, 8-800 и др.)</td><td>Текстовое поле (с ограничением на ввод только цифр)</td></tr>
</table>
– другое
</td>
<td></td>
</tr>
<tr>
<td>Дата выявления угрозы</td>
<td>Дата
Представляет собой информацию о дате выявления угрозы в формате ДД/ММ/ГГГГ. Дата выявления угрозы в случае фактической невозможности ее установления считается совпадающей с датой регистрации сообщения об уязвимости в базе данных угроз.</td>
<td>01/01/2016</td>
</tr>
<tr>
<td>Автор, опубликовавший информацию о выявленной уязвимости</td>
<td>Текстовое поле
Представляет собой информацию об авторе (участник информационного обмена/FinCERT/другое), который обнаружил и опубликовал угрозу первым. Может быть приведена ссылка на ресурс в сети интернет</td>
<td></td>
</tr>
<tr>
<td>Способ (правило) обнаружения уязвимости</td>
<td>Текстовое поле (с возможностью вложения файла)
Представляет собой формализованное правило определения реализации угрозы.
Поле должно включать в себя имя автора правила – участника информационного обмена</td>
<td></td>
</tr>
<tr>
<td>Возможные меры по устранению уязвимости</td>
<td>Текстовое поле
Предложения и рекомендации по устранению выявленных угроз или исключению возможности использования нарушителем выявленных угроз. Предложения и рекомендации должны содержать ссылки на необходимое ПО и (или) описание конфигураций ПО, для которых угрозы безопасности информации, не являются актуальными.</td>
<td></td>
</tr>
</table>

Прочая информация	Текстовое поле	

4. Типовая форма описания уязвимости (Электронная форма Уязвимости)

Название поля	**Описание поля (должно быть представлено в качестве подсказки при заполнении)**	**Пример**
Наименование уязвимости	Текстовое поле Информация об уязвимости, на основе которой возможно установить причину и (или) последствия уязвимости. Наименование уязвимости должно быть представлено на русском языке (в скобках на английском языке – при необходимости)	*Уязвимость, приводящая к переполнению буфера в службе RPC DCOM в операционных системах Microsoft Windows 4.0/2000/XP/2003 (Vulnerability Windows XP RPCSS DCOM Buffer Overflow).*
Идентификатор уязвимости	Текстовое поле (присваивается автоматически разрабатываемой системой) Представляет собой алфавитно-цифровой код, включающий код базы данных уязвимостей (FinCERT), год выявления уязвимости и порядковый номер уязвимости, выявленной в текущем году. При определении идентификатора уязвимости код базы данных уязвимостей, год выявления уязвимости и порядковый номер уязвимости должны быть отделены друг от друга знаком «-», при этом знак пробела не ставится.	*FinCERT-2016-1234*
Идентификаторы других систем описаний уязвимостей	Текстовое поле Представляет собой идентификаторы уязвимости в других системах описаний. Данный элемент включает идентификаторы уязвимости из общедоступных источников и содержит, как правило, цифровой или алфавитно-цифровой код. Описание может быть выполнено в виде гиперссылок в формате адресов URL.	*CVE ID: CVE-2003-0313*
Краткое описание уязвимости	Текстовое поле Представляет собой текстовую информацию об уязвимости и возможностях ее использования	*Уязвимость обнаружена в* службе *RPC DCOM. Нарушитель может вызвать отказ в обслуживании (аварийное завершение работы системы или перезагрузка), создавая два потока для одного и того же RPC-запроса. По сообщению разработчика, уязвимость может использоваться для выполнения произвольного кода в уязвимой системе. Разработчик оценил, что уязвимость имеет «критический» уровень опасности.*

Класс уязвимости	Текстовое поле (выбор из закрытого списка): **- Уязвимость кода** Уязвимость, появившаяся в процессе разработки программного обеспечения. **- Уязвимость конфигурации** Уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы. **- Уязвимость архитектуры** Уязвимость, появившаяся в процессе проектирования информационной системы. **- Организационная уязвимость** Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственными за защиту информации. **- Многофакторная уязвимость** Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов. **- Не задан** Поскольку значения поля «Класс уязвимости» могут быть получены только из одного источника (http://www.bdu.fstec.ru/vul), для уязвимостей, полученных из других источников (например, NVD), в автоматическом режиме будет проставляться «Не задан», с последующим изменением экспертами класса уязвимости вручную.	*Уязвимость кода*
Наименование программного обеспечения и его версия	Текстовое поле Представляет собой информацию о наименовании ПО и его версии.	*RPC/DCOM Microsoft Windows 4.0/200C/XP/2003.*
Служба (порт), которую(ый) используется для функционирования программного обеспечения	Текстовое поле Представляет собой комбинированную информацию о службе (системной или сетевой), о сетевом порте, который используется для функционирования ПО и о наименовании сетевого протокола передачи данных. Номер сетевого порта и наименование сетевого протокола передачи данных отделяют друг от друга знаком «/».	*RPC 139/tcp*

Тип недостатка	Текстовое поле (выбор из закрытого списка) ***– недостатки, связанные с неправильной настройкой параметров ПО*** Неправильная настройка параметров ПО заключается в отсутствии необходимого параметра, присвоении параметру неправильных значений, назначении избыточного числа параметров или неопределенных параметров ПО. ***– недостатки, связанные с неполнотой проверки вводимых (входных) данных*** Недостаточность проверки вводимых (входных) данных заключается в отсутствии проверки значений, избыточном количестве значений, неопределенности значений, вводимых (входных) данных. ***– недостатки, связанные с возможностью прослеживания пути доступа к каталогам*** Прослеживание пути доступа к каталогам заключается в отслеживании пути доступа к каталогу (по адресной строке/составному имени) и получении доступа к предыдущему/корневому месту хранения данных. ***– недостатки, связанные с возможностью перехода по ссылкам*** Переход по ссылкам связан с возможностью внедрения нарушителем ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Для файловых систем недостатками являются символьные ссылки и возможности прослеживания по ним нахождения ресурса, доступ к которому ограничен. ***– недостатки, связанные с возможностью внедрения команд ОС*** Внедрение команд ОС заключается в возможности выполнения пользователем команд операционной системы (например, просмотре структуры каталогов, копирование, удаление файлов и другие команды). ***– недостатки, связанные с межсайтовым скриптингом (выполнением сценариев)*** Межсайтовый скриптинг обычно распространен в веб-приложениях и позволяет внедрять код в веб-страницы, которые могут просматривать нелегитимные пользователи. Примерами такого кода являются скрипты, выполняющиеся на стороне пользователя. ***– недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки*** Недостатки связаны с внедрением интерпретируемых операторов языков программирования (например, операции выбора, добавления, удаления и другие) или разметки в исходный код веб-приложения. ***– недостатки, связанные с внедрением произвольного кода***	*недостатки, связанные с переполнением буфера памяти.*

	Недостатки связаны с внедрением произвольного кода и части кода, которые могут привести к нарушению процесса выполнения операций. ***– недостатки, связанные с переполнением буфера памяти*** Переполнение буфера возникает в случае, когда ПО осуществляет запись данных за пределами выделенного в памяти буфера. Переполнение буфера обычно возникает из-за неправильной работы с данными, полученными извне, и памятью, при отсутствии защиты со стороны среды программирования и операционной системы. В результате переполнения буфера могут быть испорчены данные, расположенные следом за буфером или перед ним. Переполнение буфера может вызывать аварийное завершение или зависание ПО. Отдельные виды переполнений буфера (например, переполнение в стековом кадре) позволяет нарушителю выполнить произвольный код от имени ПО и с правами учетной записи, от которой она выполняется. ***– недостатки, связанные с неконтролируемой форматной строкой*** Форматная строка в языках C/C++ является специальным аргументом функции с динамически изменяемым числом параметров. Ее значение в момент вызова функции определяет фактическое количество и типы параметров функции. Ошибки форматной строки потенциально позволяют нарушителю динамически изменять путь исполнения программ, в ряде случаев - внедрять произвольный код. ***– недостатки, связанные с вычислениями*** К недостаткам, связанным с вычислениями относятся следующие: • некорректный диапазон, когда ПО использует неверное максимальное или минимальное значение, которое отличается от верного на единицу в большую или меньшую сторону; • ошибка числа со знаком, когда нарушитель может ввести данные, содержащие отрицательное целое число, которые программа преобразует в положительное нецелое число; • ошибка усечения числа, когда часть числа отсекается (например, вследствие явного или неявного преобразования, или иных переходов между типами чисел); • ошибка индикации порядка байтов в числах, когда в ПО смешивается порядок обработки битов (например, обратный и прямой порядок битов), что приводит к неверному числу в содержимом, имеющем критическое значение для безопасности. ***– недостатки, приводящие к утечке/раскрытию информации ограниченного доступа*** Утечка информации - преднамеренное или неумышленное разглашение информации	

	ограниченного доступа (например, существует утечки информации при генерировании ПО сообщения об ошибке, которое содержит сведения ограниченного доступа). Недостатки, приводящие к утечке/раскрытию информации ограниченного доступа, могут быть образованы вследствие наличия иных ошибок (например, ошибок, связанных с использованием скриптов). ***– недостатки, связанные с управлением полномочиями (учетными данными)*** К недостаткам, связанным с управлением полномочиями (учетными данными) относятся, например, нарушение политики разграничения доступа, отсутствие необходимых ролей пользователей. Ошибки при удалении ненужных ученых данных и другие. ***– недостатки, связанные с управлением разрешениями, привилегиями и доступом*** К недостаткам, связанным с управлением разрешениями, привилегиями и доступом относятся, например, превышение привилегий и полномочий, необоснованному наличию суперпользователей в системе, нарушение политики разграничения доступа и другие. ***– недостатки, связанные с аутентификацией*** К недостаткам, связанным с аутентификацией относятся: возможность обхода аутентификации, ошибки логики процесса аутентификации, отсутствие запрета множественных попыток аутентификации, отсутствие требования аутентификации для выполнения критичных функций. ***– недостатки, связанные с криптографическими преобразованиями (недостатки шифрования)*** К недостаткам, связанным с криптографическими преобразованиями относятся ошибки хранения информации в незашифрованном виде, ошибки при управлении ключами, использование несертифицированных средств криптографической защиты информации. ***– недостатки, связанные с подменой межсайтовых запросов*** Подмена межсайтового запроса заключается в том, что используемое ПО не осуществляет или не может осуществить проверку корректности формирования запроса. ***– недостатки, приводящие к «состоянию гонки»*** «Состояние гонки» - ошибка проектирования многопоточной системы или приложения, при котором функционирование системы или приложения зависит от порядка выполнения части кода. «Состояние гонки» является специфической ошибкой, проявляющейся в случайные моменты времени. ***– недостатки, связанные с управлением ресурсами***	

	К недостаткам управления ресурсами относятся: недостаточность мер освобождения выделенных участков памяти после использования, что приводит к сокращению свободных областей памяти, отсутствие очистки ресурса и процессов от сведений ограниченного доступа перед повторным использованием и другие. ***– иные типы недостатков***	
Место возникновения (проявления) уязвимости	Текстовое поле (выбор из закрытого списка) **– Общесистемное (общее) программное обеспечение** **– Прикладное программное обеспечение** **– Специальное программное обеспечение** **– Технические средства** **– Портативные технические средства** **– Сетевое (коммуникационное, телекоммуникационное) оборудование** **– Средства защиты информации**	*Общесистемное (общее) программное обеспечение*
Наименование операционной системы и ином окружении уязвимого ПО	Текстовое поле Представляет собой информацию об операционной системе и ином окружении уязвимого ПО.	*Microsoft Windows 4.0/2000/XP/2003 (*32).*
Дата выявления уязвимости	Дата Представляет собой информацию о дате выявления уязвимости в формате ДД/ММ/ГГГГ. Дата выявления уязвимости в случае фактической невозможности ее установления считается совпадающей с датой регистрации сообщения об уязвимости в базе данных уязвимостей.	*01/01/2016*
Автор, опубликовавший информацию о выявленной уязвимости	Текстовое поле Представляет собой информацию об авторе, который обнаружил и опубликовал уязвимость первым. Может быть приведена ссылка на ресурс в сети интернет	
Способ (правило) обнаружения уязвимости	Текстовое поле (с возможностью вложения файла) Представляет собой формализованное правило определения уязвимости. Способ (правило) обнаружения уязвимости позволяет при помощи специальной процедуры провести проверку наличия уязвимости.	
Критерии опасности уязвимости	Текстовое поле CVSS - общая система оценки уязвимости опубликована на официальном сайте сообщества FIRST по адресу URL: http://www.first.org/cvss	*AV.H/AC:UAu:N/C:CJ\:CJA:C*

Возможные меры по устранению уязвимости	Текстовое поле Предложения и рекомендации по устранению выявленных уязвимостей или исключению возможности использования нарушителем выявленных уязвимостей. Предложения и рекомендации должны содержать ссылки на необходимое ПО и (или) описание конфигураций ПО, для которых угрозы безопасности информации, использующие данную уязвимость, не являются актуальными.	
Прочая информация	Текстовое поле	

5. Сведения, содержащиеся в карточке инцидента кода PUB (Электронная форма Публикации)

Информация направляется не позднее одного рабочего дня до проведения соответствующего мероприятия.

№ п\п	**Содержание**	**Примечание**
1	Название участника информационного обмена (обязательно)	Указывается полное официальное наименование участника обмена
2	Контактные данные ответственных лиц участника информационного обмена (обязательно)	Указывается ФИО, должность, номер телефона в формате +7XXX-XXX-XXXX (указать город) и адрес электронной почты
3	Дата и время планируемых мероприятий (обязательно)	Дата указывается в формате ГГГГММДД. Время указывается в формате ЧЧ:ММ с указанием часового пояса в формате UTC+X (например, для Москвы: UTC + 3)
4	Место проведения мероприятия (обязательно)	В соответствии с Общероссийским классификатором объектов административно-территориального деления (ОКАТО) указывается первый уровень классификации в формате **XX**
5	Дополнительные сведения по мероприятию (обязательно)	Участник может указать любые дополнительные сведения, связанные с мероприятием, которые он сочтет нужным добавить ***Заполняется в свободной форме***
6	Предпринятые действия по организации мероприятия (обязательно)	Указать, какие меры были предприняты участником для организации мероприятия. ***Заполняется в свободной форме. Если меры не принимались, указать «не принимались»***

7	Тип планируемого мероприятия (обязательно)	1) Конференция Код (**CNF**) 2) Публикация на внешнем ресурсе (в т.ч. печатные издания) Код (**PBE**) 3) Публикация на собственном ресурсе направляющего информацию (в т.ч. печатные издания) Код (**PBI**)
8	Название планируемого мероприятия или ресурса, на котором планируется раскрытие информации (обязательно)	1) Название Код (**TTL**) **Дополнительно указывается название мероприятия или адрес ресурса в информационно-телекоммуникационной сети Интернет, либо печатного издания, в свободном формате** 2) Планируемая дата опубликования (выступления) **Указывается в свободной форме**
9	Текст к планируемому мероприятию (обязательно)	***Указывается в свободной форме, либо в виде текстового файла в формате .doc***