ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

УТВЕРЖДЁН

ФСТЭК России 26 июня 2018 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

РЕГЛАМЕНТ ВКЛЮЧЕНИЯ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ В БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ

2018

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России разработан в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и направлен на реализацию Положения о банке данных угроз безопасности информации, утвержденного приказом ФСТЭК России от 16 февраля 2015 г. № 9 (зарегистрирован Минюстом России 17 апреля 2015 г., рег. № 36901).

1.2. Регламент определяет порядок взаимодействия ФАУ «ГНИИИ ПТЗИ ФСТЭК России», обеспечивающего функционирование банка данных угроз безопасности информации (далее – Оператор), с разработчиками и производителями программного обеспечения и программно-аппаратных средств (далее – изготовители), с организациями и специалистами, которые выявляют (обнаруживают) уязвимости программного обеспечения и программно-аппаратных средств (далее – исследователи), при включении информации об уязвимостях программного обеспечения и программно-аппаратных средств (далее – уязвимости) в банк данных угроз безопасности информации ФСТЭК России (далее – Банк данных угроз).

1.3. В рамках взаимодействия Оператор может заключить с изготовителем соглашение о неразглашении информации об уязвимостях, поступающей от изготовителя, с учетом положений настоящего Регламента.

2. ПОЛУЧЕНИЕ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ

2.1. Сведения об уязвимостях могут быть получены Оператором:

при поступлении информации об уязвимостях от изготовителей;

при поступлении информации об уязвимостях от исследователей;

при выполнении исследований по заданию ФСТЭК России.

2.2. Информация об уязвимости направляется в Банк данных угроз через раздел «Обратная связь» (bdu.fstec.ru) или на адрес электронной почты webmaster@bdu.fstec.ru. В информации об уязвимости указываются следующие сведения:

наименование уязвимости и ее описание;

наименование и версии уязвимого программного обеспечения или программно-аппаратного средства;

разработчик/производитель (вендор) уязвимого программного обеспечения или программно-аппаратного средства (при наличии);

тип и идентификатор ошибки в соответствии с общим перечнем ошибок CWE;

наименования операционных систем и типов аппаратных платформ, для которых актуальна уязвимость;

базовый вектор и степень опасности[1] уязвимости в соответствии с CVSS v.3.0;

порядок проверки уязвимости и подтверждающие материалы (PoC-код, видеодемонстрация или иные);

контактные данные изготовителя (наименование организации и адрес места ее нахождения, должность, фамилию, имя, отчество (при наличии) руководителя организации, наименование подразделения, ответственного за устранение уязвимостей, номер телефона, адрес электронной почты) или исследователя (имя, адрес электронной почты и (или) номер телефона).

2.3. Информация об уязвимости может направляться с использованием PGP-ключей, размещенных в разделе «Обратная связь» Банка данных угроз.

3. ОБРАБОТКА ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ

3.1. Обработка информации об уязвимостях, поступившей от изготовителей

3.1.1. Изготовитель при выявлении уязвимости в своем программном обеспечении или программно-аппаратном средстве направляет информацию о выявленной уязвимости в Банк данных угроз в соответствии с пунктом 2.2 настоящего Регламента в течение 3 рабочих дней с даты ее выявления.

В случае если изготовитель получил информацию об имеющейся в его программном обеспечении (программно-аппаратном средстве) потенциальной уязвимости из внешнего источника (в том числе от исследователей в соответствии с пунктом 3.2.1 настоящего Регламента), то информация об

[1] В соответствии с ГОСТ Р 56545 – 2015 степень опасности уязвимости может принимать одно из четырех значений; критический (оценка по CVSS – 10), высокий (оценка по CVSS – 7-9,9), средний (оценка по CVSS – 4-6,9), низкий (оценка по CVSS – 0-3,9)

уязвимости направляется изготовителем в Банк данных угроз после предварительной проверки и оценки степени опасности данной потенциальной уязвимости. Информация об уязвимости, полученная от исследователя, направляется с указанием контактных данных исследователя, выявившего уязвимость, для учета при определении рейтинга исследователя в соответствии с пунктом 4.3 настоящего Регламента (при наличии согласия исследователя на предоставление таких данных).

Рекомендуемый срок предварительной проверки и оценки степени опасности потенциальной уязвимости не должен превышать 5 рабочих дней с даты получения (опубликования) информации о наличии потенциальной уязвимости.

3.1.2. При получении от изготовителя информации об уязвимости или потенциальной уязвимости Оператор в срок не более 3 рабочих дней проверяет наличие сведений о ней в Банке данных угроз, а также в иных базах данных уязвимостей и общедоступных источниках и в случае отсутствия в них информации резервирует для уязвимости (потенциальной уязвимости) временный идентификатор (BDU-Z-XXXX-xxxxx) Банка данных угроз.

Информация о зарезервированном временном идентификаторе для уязвимости (потенциальной уязвимости) направляется изготовителю на указанный им адрес электронной почты.

При наличии информации об уязвимости (потенциальной уязвимости) в Банке данных угроз Оператор информирует об этом изготовителя и при необходимости уточняет описание уязвимости в Банке данных угроз. В случае наличия информации об уязвимости (потенциальной уязвимости) в других общедоступных базах данных уязвимостей или источниках Оператор в течение 3 рабочих дней присваивает уязвимости постоянный идентификатор (BDU-XXXX- xxxxx), во взаимодействии с изготовителем формирует описание уязвимости, образец которого приведен в приложении № 1 к настоящему Регламенту,
и размещает его в Банке данных угроз.

Информация об уязвимости в сертифицированном по требованиям безопасности информации программном обеспечении или программно-аппаратном средстве в течение 1 рабочего дня с даты получения направляется Оператором в центральный аппарат ФСТЭК России на адрес электронной почты otd24@fstec.ru для сопровождения работ изготовителя по устранению

уязвимости в сертифицированном программном обеспечении или программно-аппаратном средстве.

3.1.3. Изготовитель в отношении уязвимости, для которой Оператором зарезервирован временный идентификатор, разрабатывает меры, обеспечивающие устранение этой уязвимости (например, разработка патча, выпуск новой версии), или принимает правовые, организационные, технические меры, снижающие возможность эксплуатации уязвимости нарушителем (далее - меры по устранению уязвимости).

В отношении потенциальной уязвимости, для которой Оператором зарезервирован временный идентификатор, изготовитель проводит исследования с целью подтверждения ее актуальности и уточнения степени опасности, после чего разрабатывает меры по устранению уязвимости.

В отношении уязвимости (потенциальной уязвимости) критического или высокого уровня опасности рекомендуемый срок разработки мер по ее устранению (включая подтверждение актуальности) не должен превышать 30 рабочих дней с момента выявления уязвимости изготовителем или получения данных об уязвимости из внешних источников.

В отношении уязвимости (потенциальной уязвимости) среднего или низкого уровня опасности рекомендуемый срок разработки мер по ее устранению (включая подтверждение актуальности) не должен превышать 60 рабочих дней с момента выявления уязвимости изготовителем или получения данных об уязвимостях из внешних источников.

В случае если в результате проведения исследований потенциальной уязвимости изготовителем не подтверждается ее актуальность, информация об этом направляется в Банк данных угроз. Оператор при получении указанной информации отменяет зарезервированный временный идентификатор потенциальной уязвимости, о чем информирует изготовителя.

3.1.4. После разработки мер по устранению уязвимости в соответствии с пунктом 3.1.3 настоящего Регламента изготовитель направляет уточненную информацию об уязвимости, для которой зарезервирован временный идентификатор, и состав мер по устранению уязвимости в Банк данных угроз.

Оператор при получении уточненной информации об уязвимости от изготовителя формирует описание уязвимости, образец которого приведен в приложении № 1 к настоящему Регламенту, согласовывает описание уязвимости

с изготовителем, после чего размещает описание уязвимости в Банке данных угроз с присвоением постоянного идентификатора (BDU-XXXX-xxxxx).

Описание уязвимости критического или высокого уровня опасности размещается в Банке данных угроз не позднее 5 рабочих дней с момента получения информации об уязвимости от изготовителя.

Описание уязвимостей среднего или низкого уровня опасности размещается в Банке данных угроз не позднее 7 рабочих дней с момента получения информации об уязвимости от изготовителя.

3.1.5. Дополнительная информация об уязвимости направляется изготовителем в Банк данных угроз через раздел «Обратная связь» или на адрес электронной почты webmaster@bdu.fstec.ru. Оператор при получении дополнительной информации в течение 1 рабочего дня вносит изменения в описание уязвимости.

3.2. Обработка информации об уязвимостях, поступившей от исследователей[2]

3.2.1. При выявлении уязвимости исследователем информацию о ней рекомендуется направлять изготовителю программного обеспечения или программно-аппаратного средства, в котором выявлена эта уязвимость, для ее проверки и принятия мер по устранению.

В случае отсутствия ответа в течение 5 рабочих дней, исследователю рекомендуется повторно направить уведомление об уязвимости изготовителю.

Одновременно с направлением информации об уязвимости изготовителю она может быть направлена в Банк данных угроз в соответствии с пунктом 2.2 настоящего Регламента.

Информация об уязвимости в сертифицированном по требованиям безопасности информации программном обеспечении или программно-аппаратном средстве дополнительно направляется в центральный аппарат ФСТЭК России на адрес электронной почты otd24-bdu@fstec.ru для сопровождения работ изготовителя по устранению уязвимости в сертифицированном программном обеспечении или программно-аппаратном средстве.

---

[2] Информация об уязвимостях, выявленных исследователями на основании заданий заказчиков, может быть представлена в Банк данных угроз только по согласованию с соответствующими заказчиками.

3.2.2. При невозможности получить контактные данные службы технической поддержки изготовителя, а также в случае непринятия изготовителем мер по устранению уязвимости, исследователю рекомендуется направить информацию об уязвимости в Банк данных угроз в соответствии с пунктом 2.2 настоящего Регламента.

При этом непринятием мер по устранению уязвимости считается:

отсутствие в течение 5 рабочих дней ответа на повторное уведомление об уязвимости или на иной последующий запрос, направленный изготовителю;

отказ от взаимодействия по подтверждению или устранению уязвимости, выраженный в устной или письменной форме;

отсутствие опубликованных в Банке данных угроз мер по устранению уязвимости в течение 60 рабочих дней с момента предоставления информации исследователем.

3.2.3. При поступлении информации об уязвимости от исследователя Оператор в срок не более 3 рабочих дней в отношении уязвимости критического или высокого уровня опасности и 5 рабочих дней в отношении уязвимости среднего или низкого уровня опасности проверяет наличие сведений о выявленной уязвимости в Банке данных угроз, а также в иных общедоступных базах данных уязвимостей и источниках.

При наличии информации о выявленной уязвимости в Банке данных угроз Оператор информирует об этом исследователя и при необходимости уточняет описание уязвимости в Банке данных угроз. В случае наличия информации об уязвимости в других общедоступных базах данных уязвимостей или источниках Оператор информирует об этом исследователя, присваивает уязвимости постоянный идентификатор (BDU-XXXX-xxxxx), формирует описание уязвимости и размещает его в Банке данных угроз.

Информация об уязвимости в сертифицированном по требованиям безопасности информации программном обеспечении или программно-аппаратном средстве в течение 1 рабочего дня с даты получения направляется Оператором в центральный аппарат ФСТЭК России на адрес электронной почты otd24-bdu@fstec.ru для сопровождения работ изготовителя по устранению уязвимости в сертифицированном программном обеспечении или программно-аппаратном средстве.

3.2.4. При отсутствии в Банке данных угроз или в иных общедоступных базах данных уязвимостей (источниках информации) информации об уязвимости

Оператор при наличии контактных данных направляет в службу технической поддержки изготовителя уведомление об уязвимости и запрашивает контактные данные лиц изготовителя, которым необходимо предоставить полную информацию о выявленной уязвимости.

В случае отсутствия ответа в течение 5 рабочих дней Оператор повторно направляет уведомление об уязвимости изготовителю.

При получении ответа Оператор направляет изготовителю имеющуюся информацию о потенциальной уязвимости для ее проверки, а также информацию об исследователе, выявившем уязвимость (в случае наличия согласия исследователя на предоставление информации).

При необходимости Оператор организует взаимодействие изготовителя с исследователем, выявившим уязвимость, с целью подтверждения наличия уязвимости и разработки мер по ее устранению.

3.2.5. Изготовитель при получении информации об уязвимости от Оператора проверяет ее и в случае подтверждения наличия такой уязвимости направляет уточненную информацию Оператору.

3.2.6. Оператор при получении подтверждения об уязвимости от изготовителя резервирует для уязвимости временный идентификатор (BDU-Z- XXXX-xxxxx), о чем информирует изготовителя.

Дальнейшее взаимодействие Оператора и изготовителя осуществляется в соответствии с пунктами 3.1.2 - 3.1.5 настоящего Регламента.

3.2.7. При невозможности получить контактные данные службы технической поддержки изготовителя, а также в случае непринятия изготовителем мер по устранению уязвимости, Оператор проводит самостоятельные исследования с целью подтверждения наличия уязвимости в программном обеспечении или программно-аппаратном средстве.

При этом непринятием мер по устранению уязвимости считается:

отсутствие в течение 5 рабочих дней ответа на повторное уведомление об уязвимости или на иной последующий запрос, направленный Оператором;

отказ от взаимодействия с Оператором в соответствии с пунктами 3.1.2 - 3.1.5 настоящего Регламента.

Срок проведения Оператором исследований уязвимости не должен превышать 60 рабочих дней с даты получения информации от исследователя. В зависимости от сложности уязвимого программного обеспечения или

программно-аппаратного средства указанный срок может быть продлен по согласованию с ФСТЭК России.

Исследования могут проводиться во взаимодействии с исследователем, направившим информацию об уязвимости.

Для проведения исследований Оператором на основе соглашения могут привлекаться экспертные организации, которые являются участниками ведения Банка данных угроз (организации-участники Банка данных угроз)[3]. Информация об уязвимости, исследуемой организацией-участником Банка данных угроз, не подлежит раскрытию.

3.2.8. При подтверждении по результатам исследований, проведенных в соответствии с пунктом 3.2.7 настоящего Регламента, наличия уязвимости в программном обеспечении или программно-аппаратном средстве Оператор присваивает уязвимости постоянный идентификатор, во взаимодействии с исследователем, направившим информацию об уязвимости, формирует описание уязвимости, образец которого приведен в приложении № 1 к настоящему Регламенту, и размещает его в Банке данных угроз.

4. РАСКРЫТИЕ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ

4.1. Раскрытие информации об уязвимости осуществляется путем размещения Оператором описания уязвимости в Банке данных угроз.

4.2. Раскрытие информации об уязвимости в Банке данных угроз осуществляется в случае, если:

информация об уязвимости опубликована в иных общедоступных базах данных уязвимостей или источниках;

информации об уязвимости и мерах по ее устранению получена от изготовителя в соответствии с настоящим Регламентом;

изготовитель не принимает меры по устранению уязвимости в соответствии с настоящим Регламентом;

отсутствуют контактные данные изготовителя или его службы технической поддержки.

4.3. Оператор на основании информации об уязвимостях, представленных исследователями, ведет рейтинг исследователей («доску почета») и размещает его на сайте Банка данных угроз (в случае наличия согласия исследователей

[3] Перечень организаций, являющихся участниками ведения Банка данных угроз, размещен в разделе «Участники/организации» сайта bdu.fstec.ru.

размещение такой информации). Рейтинг определяется в соответствии с приложением № 2 к настоящему Регламенту путем расчета баллов, присвоенных исследователю за предоставленную информацию о не известных ранее уязвимостях и опубликованную в Банке данных угроз.

4.4. Исследователям, выявившим уязвимость, не рекомендуется раскрывать информацию об уязвимостях без согласования с изготовителем или Оператором.

Приложение № 1
к Регламентувключения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России

Описание
уязвимости для размещения в Банке данных угроз

BDU: XXXX-xxxxx: Наименование уязвимости

Описание уязвимости	
Наименование уязвимого программного обеспечения	
Версия уязвимого программного обеспечения	
Производитель/разработчик (вендор)	
Наименование операционной системы и типа аппаратной платформы, для которых актуальна уязвимость	
Тип Ошибки (идентификатор)	
Класс уязвимости	
Дата выявления уязвимости	
Базовый вектор уязвимости	
Уровень опасность уязвимости	
Возможные меры по устранению уязвимости	
Статус уязвимости	
Наличие «эксплойта»	
Способ эксплуатации	

Способ устранения	
Информация об устранении уязвимости	
Источники, в которых опубликованы сведения об уязвимости	
Идентификаторы уязвимости в иных системах описаний	
Прочая информация об уязвимости	

Приложение № 2
к Регламенту включения информации об
уязвимостях программного обеспечения и
программно-аппаратных средств банк данных
угроз безопасности информации
ФСТЭК России

Определение
рейтинга исследователей, предоставивших информацию об уязвимостях в Банк данных угроз

Исследователь получает рейтинговые баллы за предоставленные сведения об уязвимостях в Банк данных угроз безопасности при выполнении следующих условий:

1) сведения об уязвимости не опубликованы ранее в Банке данных угроз или других общедоступных источниках;

2) исследователем представлены информация об уязвимости и контактная информация исследователя в соответствии с Регламентом обращения с информацией об уязвимостях программного обеспечения и программно-аппаратных средств в Банке данных угроз безопасности информации ФСТЭК России.

Количество рейтинговых баллов за выявленную уязвимость определяется по следующей формуле:

$A = (T + P + R) * C$, где

T – показатель, характеризующий объект исследований (выбирается тип программного обеспечения с максимальным значением);

P – показатель, характеризующий алгоритм проверки уязвимости и подтверждающие материалы;

R – показатель, характеризующий уровень опасности уязвимости;

C – показатель, характеризующий количество затрагиваемого программного обеспечения.

Общий рейтинг исследователя определяется простым суммированием всех рейтинговых баллов, полученных исследователем за информацию об уязвимостях, сведения о которых были представлены в Банк данных угроз.

Значения показателей при определении рейтинга:

Критерии	**Значения**	**Баллы**
Показатель, характеризующий объект исследований (**T**)	Встроенное программное (микропрограммное) обеспечение, программное обеспечение телекоммуникационного оборудования, программное обеспечение средств защиты информации	10
	Общесистемное программное обеспечение (в том числе программное обеспечение виртуализации), программное обеспечение автоматизированных систем управления технологическими процессами	7
	Прикладное программное обеспечение (в том числе системы управления базами данных**)**	5
Показатель, характеризующий алгоритм проверки уязвимости и подтверждающие материалы (**P**)	Разработан PoC или представлен алгоритм действий	3
	Представлено видеоподтверждение	2
	Прочие методы	1
Показатель, характеризующий уровень опасности уязвимости (**R)**	Определяется в соответствии с оценкой CVSS v.3.0: критический (10) высокий (7-9,9); средний (4-6,9); низкий (0-3,9)	 10 7 3 1
Показатель количества затрагиваемого уязвимостью ПО (**C**)	Уязвимость актуальна для нескольких типов программного обеспечения (множественная уязвимость)	1,5
	Уязвимость актуальна только для одного типа программного обеспечения	1,0

В случае если исследователем дополнительно представлено описание уязвимости на языке OVAL, то к общему количеству рейтинговых баллов, рассчитанному по приведенной выше формуле, прибавляется дополнительно 2 балла.

Максимальное возможное количество рейтинговых баллов за одну уязвимость **- 36,5.**

Минимальное возможное количество рейтинговых баллов за одну уязвимость **- 7.**