**ФЕДЕРАЛЬНЫЙ ИНТЕРНЕТ-ЭКЗАМЕН ДЛЯ ВЫПУСКНИКОВ БАКАЛАВРИАТА И СПЕЦИАЛИТЕТА (ФИЭБ)**

**НАПРАВЛЕНИЕ ПОДГОТОВКИ**
**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**ПРИМЕРЫ ЗАДАНИЙ ПИМ**

# ЧАСТЬ 1 ПИМ

**Дисциплина «Безопасность жизнедеятельности»**
**Задание** (укажите не менее двух вариантов ответов)

Авария – это происшествие в технической системе …

*Варианты ответов:*
1) сопровождающееся разрушением биосферы
2) при котором невозможно или нецелесообразно восстановление технических средств
3) сопровождающееся гибелью людей
4) не сопровождающееся гибелью людей

**Дисциплина «Защита и обработка конфиденциальных документов»**
**Задание** (укажите не менее двух вариантов ответов)

Согласно современному российскому законодательству, юридическая сила электронного документа удостоверяется с помощью …

*Варианты ответов:*
1) удостоверяющего письма, составленного создателем документа на машинном носителе
2) бумажного аналога отправленного по электронной почте документа
3) регистрационного индекса
4) электронной цифровой подписи

**Дисциплина «Математическая логика и теория алгоритмов»**
**Задание** (укажите не менее двух вариантов ответов)

Классическая логика основывается на принципе, согласно которому каждое высказывание либо истинно, либо ложно. Это так называемый *принцип двузначности*, который подразумевает, что …

*Варианты ответов:*
1) всякое высказывание имеет одно (и только одно) из трех или более истинностных значений
2) каждое утверждение либо истинно, либо ложно
3) нельзя объявлять одно и то же суждение истинным и ложным
4) суждение имеет одно из двух возможных истинностных значений – «истинно» и «ложно»

**Дисциплина «Организационно-правовое обеспечение информационной безопасности»**
**Задание** (укажите не менее двух вариантов ответов)

К признакам защищаемой информации как объекта правового регулирования относятся …

*Варианты ответов:*

1) степень секретности
2) массовость
3) принадлежность
4) содержание
5) достоверность

**Дисциплина «Программно-аппаратные средства защиты информации»**
**Задание** (введите ответ в поле)

Документ, подтверждающий, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, называется аттестатом … (Введите слово в форме соответствующего падежа.)

*Введите ответ*

**Дисциплина «Техническая защита информации»**
**Задание** (введите ответ в поле)

В основе системного подхода к защите информации лежат следующие методы обработки, хранения и передачи информации …

*Варианты ответов:*

1) организационные
2) политические
3) программно-технические
4) физические
5) психолого-диагностические

**Дисциплина «Технологии и методы программирования»**
**Задание** (установите правильную последовательность в предложенной совокупности ответов)

Установите правильную последовательность расположения операторов фрагмента программы для решения задачи вывода на экран суммы максимальных значений строк вещественной матрицы **t** размером n × m (n <= 10, m <= 100 – исходные данные).

*Варианты ответов:*

1) if (t[i][j] > max)
2) float t[10][100], max, sum = 0; int i, j;
3) max = t[i][j];
4) for (i = 0; i < 10; i++)
5) }
6) for (j = 0; j < 100; j++)
7) printf ("\n %f", sum);
8) sum = sum + max;
9) { max = t[i][0];

**Дисциплина «Управление информационной безопасностью»**
**Задание** (элементы доступны для перетаскивания)

Установите соответствие между целями обеспечения информационной безопасности и их содержанием.

1. Конфиденциальность –

2. Целостность – _____

3. Доступность – _____

*Варианты ответов:*

1) отсутствие неправомочных искажений, добавлений или уничтожения информации
2) обеспечение своевременного и надежного доступа к информации и информационным сервисам
3) состояние доступности информации только авторизованным пользователям, процессам и устройствам
4) возможность однозначно идентифицировать автора или источник информации

**Дисциплина «Электроника и схемотехника»**

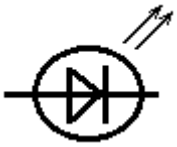
**Задание** (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Установите соответствие между полупроводниковым прибором и его условным обозначением.

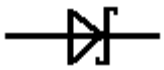
1. Диод
2. Стабилитрон
3. Диод Шоттки
4. Варикап

*Варианты ответов:*

1) 

2) 

3) 


4) 

5) 

# ЧАСТЬ 2 ПИМ

**Кейс-задание**
**(Тип задач профессиональной деятельности: экспериментально-исследовательский)**

**Задание**
Важным компонентом базы данных угроз (БДУ) Федеральной службы по техническому и экспортному контролю (ФСТЭК) является каталог уязвимостей. Данный каталог обновляется один раз или два раза в год. Каталог хорошо структурирован, имеет сквозную нотацию, а общее число описанных угроз постоянно увеличивается. Согласно описанию БДУ ФСТЭК, угрозы безопасности информации, включенные в состав банка данных угроз, не являются элементами иерархической классификационной системы угроз, а представляют собой обобщенный перечень основных угроз безопасности информации, потенциально опасных для информационных систем.
Необходимо предложить исходный алгоритм использования БД угроз ФСТЭК России для определения алгоритма действий по включению новой угрозы информационной безопасности информационных (автоматизированных) систем и их систем защиты.

| Краткое содержание информации | Имя файла | Скачать файл | |
|---|---|---|---|
| Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России | 1k3_Pril1 | PDF | DOC |
| Оценка уязвимостей CVSS 3.0 | 1k3_Pril2 | PDF | DOC |

**Подзадача 1** (укажите не менее двух вариантов ответов)

Банк данных угроз безопасности информации предназначен для заказчиков, операторов, разработчиков информационных (автоматизированных) систем и их систем защиты, разработчиков и производителей средств защиты информации, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

Банк данных угроз безопасности информации содержит сведения о (об) …

*Варианты ответов:*

1) рисках информационной безопасности критически важных объектов информационной инфраструктуры организации

2) уязвимостях, в первую очередь характерных для государственных информационных систем

3) уязвимостях испытательных лабораторий и органов по сертификации средств защиты информации

4) основных угрозах безопасности информации

5) уязвимостях автоматизированных систем управления производственными и технологическими процессами критически важных объектов

**Подзадача 2** (укажите не менее двух вариантов ответов)

Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России 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).
Сведения об уязвимостях могут быть получены Оператором …
*При решении задания используйте файл 1k3_Pril1.*

Банк данных угроз безопасности информации содержит сведения о (об) …

*Варианты ответов:*

1) при поступлении информации об уязвимостях от изготовителей

2) при поступлении информации об уязвимостях, полученных в результате научных исследований, проводимых на объектах информатизации предприятий

3) при поступлении информации о нарушениях регламентов испытательных лабораторий и органов по сертификации средств защиты информации

4) при поступлении информации об уязвимостях от исследователей

5) при выполнении исследований по заданию ФСТЭК России

6) при поступлении информации с критически важных объектов информационной инфраструктуры организации

**Подзадача 3** (укажите не менее двух вариантов ответов)

Раскрытие информации об уязвимости осуществляется путем размещения описания уязвимости в банке данных угроз. В соответствии с «Регламентом включения информации об уязвимостях программного обеспечения и программно-аппаратных средств» в банк данных угроз безопасности информации ФСТЭК России, информация об уязвимостях может быть предоставлена в следующих случаях …

Банк данных угроз безопасности информации содержит сведения о (об) …

*Варианты ответов:*

1) информация об уязвимости не может быть опубликована в общедоступных базах данных уязвимостей или источниках

2) изготовитель не принимает меры по устранению уязвимости в соответствии с Регламентом

3) изготовитель предпринял меры по устранению уязвимостей в соответствии с Регламентом

4) информация об уязвимости и мерах по ее устранению получена от изготовителя в соответствии с Регламентом

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

6) информация об уязвимости и мерах по ее устранению получена от посторонних лиц

**Подзадача 4** (элементы доступны для перетаскивания)

Показатель, характеризующий уровень опасности уязвимости, определяется в соответствии с оценкой CVSS v.3.0.
Установите соответствие между уровнем опасности уязвимости и ее числовым значением.

1. Критический уровень – _____

2. Высокий уровень – _____

3. Средний уровень – _____

4. Низкий уровень – _____

*При решении задания используйте файл 1k3_Pril2.*

*Варианты ответов:*

1) 8,1
2) 10
3) 12
4) 4,2
5) 0,5

**Подзадача 5** (укажите не менее двух вариантов ответов)

База данных угроз ФСТЭК – это самый большой каталог уязвимостей. Помимо важных и полезных – базы уязвимостей и базы угроз, – сайт БДУ ФСТЭК предлагает и дополнительные инструменты.
Каталог угроз позволяет осуществлять контекстный поиск по названию угрозы и применять фильтры по …

*Варианты ответов:*

1) источникам угрозы
2) критичности реализации угрозы
3) вероятности реализации угрозы
4) последствиям реализации угрозы

**ПРИЛОЖЕНИЯ К КЕЙС-ЗАДАНИЮ**

Приложение 1k3_Pril1

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

## 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.

---

[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)

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 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.

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 соответствиис 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.

---

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

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

## 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 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.

**Справочные сведения об общей системе оценки уязвимости**

Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности.

В настоящее время наибольшее распространение в практической деятельности по оценке опасности уязвимостей получила версия 2.0 общей системы оценки уязвимостей.

Система оценки CVSS v2.0 состоит из трех групп метрик (критериев): базовых, временных и контекстных.

Группа базовых метрик (критериев) отражает аспекты опасности уязвимости, влияющие на доступность, целостность и конфиденциальность информации.

Группа временных метрик (критериев) отражает характеристики уязвимости, которые изменяются со временем (подтверждение технических параметров уязвимости, статус исправления уязвимости и доступность технологии эксплуатации), но не зависят от среды функционирования программного обеспечения.

Группа контекстных метрик (критериев) отражает характеристики уязвимости, зависящие от среды функционирования программного обеспечения.

Для осуществления комбинированной оценки уязвимостей по различным группам метрик (критериев) используются базовый, временной и контекстный векторы уязвимости.

Количественная оценка степени опасности уязвимости проводится по результатам анализа базового вектора уязвимости. Временные и контекстные векторы применяются только в тех случаях, когда возникает необходимость уточнения базового вектора.

Базовый вектор уязвимости CVSS v2.0 представляет собой комбинированную информацию о базовых метриках (критериях), представляемую в виде текстовой формализованной записи (строки) и численного значения (оценки).

Базовый вектор уязвимости имеет следующий формат:

AV:**X**/AC:**X**/Au:**X**/C:**X**/I:**X**/A:**X**, где

- AV – метрика (критерий) способа получения доступа нарушителем;
- AC – метрика (критерий) сложности получения доступа нарушителем;
- Au – метрика (критерий) характеристики потребности нарушителя в аутентификации;
- C – метрика (критерий) влияния на конфиденциальность;
- I – метрика (критерий) влияния на целостность;
- A – метрика (критерий) влияния на доступность;
- значение метрики (критерия).

Каждая метрика (критерий) может принимать одно из трех значений.

Метрика (критерий) AV может принимать следующие значения:

- L – получение физического (локального) доступа к объекту;
- A – получение доступа к объекту из локальной вычислительной сети;
- N – получение доступа к объекту из любой вычислительной сети, связанной с объектом атаки.

Метрика (критерий) AC может принимать следующие значения:

- H – для получения доступа требуется выполнение особых условий (например, повышение привилегий или получение дополнительной информации при помощи методов «социальной инженерии»);
- M – для получения доступа требуется выполнение специальных условий (например, прохождение нестандартной процедуры аутентификации или получение предварительной информации при действиях, приводящих к гарантированному результату);
- L – для получения доступа выполнение специальных условий не требуется (L).

Метрика (критерий) Au может принимать следующие значения:

- N – аутентификация не требуется;
- S – требуется однократная аутентификация;
- M – требуется многократная аутентификация.

Метрика (критерий) C может принимать следующие значения:

- N – не оказывает влияния на конфиденциальность данных;
- P – частичное нарушение конфиденциальности данных;
- C – полное нарушение конфиденциальности данных.

Метрика (критерий) I может принимать следующие значения:

- N – не оказывает влияния на целостность данных;
- P – частичное неправомерное уничтожение или модифицирование данных;
- C – полное неправомерное уничтожение или модифицирование данных.

Метрика (критерий) A может принимать следующие значения:

- N – не оказывает влияния на доступность данных;
- P – кратковременное неправомерное блокирование данных;
- C – долговременное неправомерное блокирование данных.

Численное значение базового вектора уязвимости (базовая оценка) изменяется от 0 до 10.

На основе численного значения базового вектора V уязвимости (базовой оценки) присваиваются один из четырех уровней опасности:

- низкий уровень опасности, если $0{,}0 \leq V \leq 3{,}9$;
- средний уровень опасности, если $4{,}0 \leq V \leq 6{,}9$;
- высокий уровень опасности, если $7{,}0 \leq V \leq 9{,}9$;
- критический уровень опасности, если $V = 10{,}0$.