|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДЕНО |
|  |  | Должность представителя поставщика |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
|  |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

[Наименование органиЗации]

Протокол выявления уязвимостей цифрового продукта [Наименование цифрового продукта]

Страниц \_\_

Москва

2023 г.

Исследование проводится с целью выявления уязвимостей, условий
и факторов, создающих возможность нарушения целостности объекта оценки, а также нарушения конфиденциальности, целостности и доступности обрабатываемой (защищаемой) информации в цифровом продукте [Наименование цифрового продукта].

**Содержание**

**1.** **Обозначения и сокращения**

В настоящем документе введены следующие обозначения и сокращения
на русском и английском языках.

|  |  |
| --- | --- |
| Сокращение | Описание/Определение |
| CVSS | Common Vulnerability Scoring System –  открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет ее исправления |
| NVD | National Vulnerability Database - американская база данных уязвимостей является наиболее полным общедоступным хранилищем сведений об уязвимостях |
| БДУ | Банк данных угроз безопасности информации |
| ОО | Объект оценки |
| СВТ | Средства вычислительной техники |
| СУБД | Система управления базой данных |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю Российской Федерации |

# 2. Термины и определения

В настоящем документе введены следующие термины на русском языке.

|  |  |
| --- | --- |
| Термин | Описание/Определение |
| National Vulnerability Database | Американская база данных уязвимостей является наиболее полным общедоступным хранилищем сведений об уязвимостях |

# 3. Общие положения

Объектом испытаний является цифровой продукт [Наименование цифрового продукта] (далее, в зависимости от контекста – цифровой продукт, объект оценки).

# 4. Объект оценки

[Наименование цифрового продукта] реализует следующую функциональность:

- [перечень функций цифрового продукта].

# 5. Цель анализа уязвимостей

Исследование объекта оценки по выявлению уязвимостей проводится с целью выявления условий и факторов, создающих возможность нарушения целостности объекта оценки, а также нарушения конфиденциальности, целостности и доступности обрабатываемой (защищаемой) информации.

# 6. Средства и условия проведения испытаний

## 6.1. Условия проведения испытаний

Для проведения работ по выявлению уязвимостей используются документация на объект оценки, различные публикации (разработчиков, пользователей и исследователей) по анализу функционирования объекта оценки и исследований уязвимостей в нем, дистрибутив объекта оценки, исполняемый код объекта оценки, исходный код объекта оценки.

## 6.2. Ограничения на проведение испытаний

Исследования проводятся до полной отработки всех технологических операций. В случае установления факта невозможности устранения уязвимостей
с использованием мер, предложенных разработчиком, Цифровой продукт возвращается на доработку.

Испытания проводились в нормальных климатических условиях эксплуатации СВТ в помещениях, удовлетворяющих условиям эксплуатации СВТ, в дневное время, при температуре от +20º C до +25º C. Никаких специальных мер по обеспечению давления и влажности в помещениях, отличных от условий в рабочих помещениях, не предусматривается.

Меры, обеспечивающие безопасность и безаварийность проведения испытаний, а также техническое оснащение испытательного стенда должны соответствовали, действующим нормам и правилам обеспечения безопасности работ
с вычислительной техникой.

## 6.3. Оцениваемые характеристики

При выявлении уязвимостей в Цифровом продукте оцениваются следующие исходные данные:

- документация на ОО;

- исходный текст (исходный код) объекта оценки;

- дистрибутив объекта оценки.

При проведении испытаний оцениваются:

- контроль отсутствия потенциальных уязвимостей ОО, выявляемых при анализе документации на ОО;

- контроль отсутствия потенциальных уязвимостей в ОО, полученных при поиске информации в общедоступных источниках;

- контроль отсутствия идентифицированных уязвимостей при проведении тестирования на проникновение.

## 6.4. Учитываемые возможности нарушителя

При необходимости проведения тестирования проникновения
для идентифицированных уязвимостей учитывается, что ОО должен являться стойким к нападениям, выполняемым нарушителем, обладающим Базовым возможностями по реализации угроз безопасности информации, в соответствии с «Методикой оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021 г.).

В таблице № 1 описаны возможности нарушителей по реализации угроз безопасности информации, учитываемые при исследовании ОО.

Таблица № 1 - Возможности нарушителей по реализации угроз безопасности информации

|  |  |  |
| --- | --- | --- |
| Уровень возможностей нарушителей | Возможности нарушителей по реализации угроз безопасности информации | Виды нарушителей |
| Нарушитель, обладающий базовыми возможностями  | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов  | Физическое лицо (хакер) |
| Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)  |
| Авторизованные пользователи систем и сетей  |
| Бывшие работники (пользователи)  |

# 7. Проведение исследований по выявлению уязвимостей объекта оценки

## 7.1. Анализ документации на объект оценки

**Критерий оценки**: документация разработчика должна содержать сведения
об ОО, дающие представление о функциях ОО и позволяющие определить поверхность атаки.

Эксперт осуществил анализ документации и иных исходных данных об ОО.
В ходе анализа документации разработчика об объекте оценки выполнено исследование представленной на испытания документации разработчика в составе, указанном ниже (см. Таблица № 2).

Таблица № 2 - Комплект документации

|  |
| --- |
| Наименование |
| Описание цифрового продукта (назначение, перечень основных функций, выполнение которых обеспечивает цифровой продукт) |
| Руководство пользователя  |
| Регламент эксплуатации  |
| Руководство системного администратора (приложений/баз данных) |
| Руководство по установке |

На основе представленной документации Экспертом определены структура ОО на уровне программ (файлов), программные модули, программный код, условия
и режим функционирования ОО, параметры и способы запуска объекта оценки, функциональные возможности ОО, дающих детальное представление о нем.

**Вывод:** на основе сведений сведения о функциональных возможностях, условиях и режимах функционирования, структуре на уровне файлов, сторонних компонентов программного обеспечения, Эксперт сформировал перечень внешних интерфейсов Цифрового продукта, непосредственно доступных для атаки потенциальным нарушителям, а также интерфейсы внутренних компонентов, косвенно доступных потенциальному нарушителю.

С точки зрения возможной эксплуатации потенциальных уязвимостей могут рассматриваться только те модули, которые непосредственно взаимодействуют
с источником потенциальных уязвимостей. Такими программными модулями являются модули, участвующие в сетевом взаимодействии, взаимодействующие
с пользователями, администраторами и операторами системы.

В результате анализа представленной документации потенциальных уязвимостей ОО **не выявлено**.

## 7.2. Анализ отсутствия потенциальных уязвимостей в ОО, полученных при поиске информации в общедоступных источниках

**Критерий оценки**: По результатам анализа ОО на основе открытых источников осуществляется выявление не устранённых известных уязвимостей,
а также идентификация потенциальных уязвимостей или их отсутствие.

### 7.2.1. Проведения анализа безопасности ОО на основе открытых источников.

Для пакетов, входящих в состав дистрибутива ОО, Эксперт провел поиск информации по открытым источникам о наличии в пакетах уязвимостей, и проверил применение рекомендованных исправлений для их устранения. Каждая из уязвимостей характеризуется числовым показателем по десятибалльной шкале, который характеризует ее опасность. Этот показатель называется оценкой уязвимости по стандарту CVSS. Чем выше значение показателя, тем более опасны последствия наличия данной уязвимости в программном обеспечении. Кроме того, в зависимости от значения данного показателя, уязвимости условно классифицируют по уровню значимости на следующие группы: CRITICAL, HIGH, MEDIUM и LOW. Наиболее важными с точки зрения обеспечения информационной безопасности являются уязвимости уровня CRITICAL, HIGH.

При выполнении идентификации потенциальных уязвимостей ОО с учетом открытых источников Экспертом было выполнено исследование следующих источников информации:

* банк данных угроз безопасности информации ФСТЭК России («http://bdu.fstec.ru»);
* база данных уязвимостей ПО National Vulnerability Database (https://nvd.nist.gov);
* результаты анализа ОО с использованием различных автоматизированных анализаторов (сетевых, конфигураций и т.п.).

### 7.2.2 Результаты анализа уязвимостей по открытым источникам

Поиск осуществляется в программных пакетах (содержащих исходный код)

[перечень модулей, компонент (с указанием версий), входящих в состав цифрового продукта][[1]](#footnote-2).

Результаты поиска информации об уязвимостях ОО по открытым источникам с описанием уязвимостей ОО, информацией об оценке каждой уязвимости приведены ниже (см. Таблица 3).

Таблица 3 - Статистика уязвимостей объекта оценки по уровням опасности

| Уровень уязвимости  | Количество уязвимостей |
| --- | --- |
| LOW | 0 |
| MEDIUM | 0 |
| HIGH | 4 |
| CRITICAL | 3 |
| Всего | 7 |

Результаты поиска уязвимостей по базам данных уязвимостей приведены на рисунках 1 - 4.



**Рисунок № 1 - Результаты поиска уязвимостей в БДУ ФСТЭК России (Hadoop 3.1.3)**



Рисунок 2 - Результаты поиска уязвимостей в БДУ ФСТЭК России (**Hadoop 3.1.3**)



**Рисунок 2 -№ 2 Результаты поиска уязвимостей в National Vulnerability** **Database** Database**(Hadoop 3.1.3)** (Hadoop 3.1.3)

Рисунок **2** - Результаты поиска уязвимостей

 в National Vulnerability Database (**Hadoop 3.1.3)**



**Рисунок № 3 - Результаты поиска уязвимостей в БДУ ФСТЭК России (HBASE 2.2.3)**



**Рисунок № 4** - Результаты поиска уязвимостей

 в National Vulnerability Database (**HBASE 2.2.3)**

Анализ полученных результатов показал, что для пакета **Hadoop 3.1.3**
в National Vulnerability Database найдено 6 уязвимостей: три уровня critical (CVE-2022-25168, CVE-2021-37404, CVE-2022-26612) и три уровня high (CVE-2021-25642, CVE-2021-33036, CVE-2020-9492). Детализация уязвимости, оценка ее применимости, компенсирующие меры (при необходимости) для **Hadoop 3.1.3** представлены
в таблице № 4.

Для пакета **HBASE 2.2.3** в National Vulnerability Database найдена уязвимость уровня high (CVE-2019-15544). Детализация уязвимости, оценка ее применимости, компенсирующие меры (при необходимости) для **HBASE 2.2.3** представлены
в таблице № 5.

Таблица № 4 – Информация по уязвимостям для **Hadoop 3.1.3**

| **Номер уязвимости** | **Описание уязвимости** | **Описание применимости/компенсационная мера** | **Статус** |
| --- | --- | --- | --- |
| CVE-2021-25642 | ZKConfigurationStore which is optionally used by CapacityScheduler of Apache Hadoop YARN deserializes data obtained from ZooKeeper without validation. An attacker having access to ZooKeeper can run arbitrary commands as YARN user by exploiting this. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.4 or later (containing YARN-11126) if ZKConfigurationStore is used. | Планировщик CapacityScheduler не используется. Вместо его используется Fair Scheduler | Уязвимость не применима |
| CVE-2022-25168 | Apache Hadoop's FileUtil.unTar(File, File) API does not escape the input file name before being passed to the shell. An attacker can inject arbitrary commands. This is only used in Hadoop 3.3 InMemoryAliasMap.completeBootstrapTransfer, which is only ever run by a local user. It has been used in Hadoop 2.x for yarn localization, which does enable remote code execution. It is used in Apache Spark, from the SQL command ADD ARCHIVE. As the ADD ARCHIVE command adds new binaries to the classpath, being able to execute shell scripts does not confer new permissions to the caller. SPARK-38305. "Check existence of file before untarring/zipping", which is included in 3.3.0, 3.1.4, 3.2.2, prevents shell commands being executed, regardless of which version of the hadoop libraries are in use. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.3 or upper (including HADOOP-18136). |  Не используется tar/untar | Уязвимость не применима |
| CVE-2021-33036 | In Apache Hadoop 2.2.0 to 2.10.1, 3.0.0-alpha1 to 3.1.4, 3.2.0 to 3.2.2, and 3.3.0 to 3.3.1, a user who can escalate to yarn user can possibly run arbitrary commands as root user. Users should upgrade to Apache Hadoop 2.10.2, 3.2.3, 3.3.2 or higher. | Учетная запись пользователя yarn без пароля. Запуск команд от лица этого пользователя возможен только привилегированным пользователем Цифрового продукта | Уязвимость не применима |
| CVE-2021-37404 | There is a potential heap buffer overflow in Apache Hadoop libhdfs native code. Opening a file path provided by user without validation may result in a denial of service or arbitrary code execution. Users should upgrade to Apache Hadoop 2.10.2, 3.2.3, 3.3.2 or higher. | Уязвимость эксплуатируется на клиентской стороне (не наносит вреда платформе). Компенсируется запретом использования библиотеки libhdfs до обновления Цифрового продукта до версии, где данная уязвимость устранена | Уязвимость компенсируется |
| CVE-2022-26612 | In Apache Hadoop, The unTar function uses unTarUsingJava function on Windows and the built-in tar utility on Unix and other OSes. As a result, a TAR entry may create a symlink under the expected extraction directory which points to an external directory. A subsequent TAR entry may extract an arbitrary file into the external directory using the symlink name. This however would be caught by the same targetDirPath check on Unix because of the getCanonicalPath call. However on Windows, getCanonicalPath doesn't resolve symbolic links, which bypasses the check. unpackEntries during TAR extraction follows symbolic links which allows writing outside expected base directory on Windows. This was addressed in Apache Hadoop 3.2.3 |  ОС Windows на платформе не используется. Уязвимость применима только для этой ОС | Уязвимость не применима |
| CVE-2020-9492 | In Apache Hadoop 3.2.0 to 3.2.1, 3.0.0-alpha1 to 3.1.3, and 2.0.0-alpha to 2.10.0, WebHDFS client might send SPNEGO authorization header to remote URL without proper verification. | WebHDFS клиент не используется  | Уязвимость не применима |

Таблица№ 5 – Информация по уязвимостям дл**я HBASE 2.2.3**

| **Номер уязвимости** | **Описание уязвимости** | **Описание применимости/компенсационная мера** | **Статус** |
| --- | --- | --- | --- |
| CVE-2019-15544 | An issue was discovered in the protobuf crate before 2.6.0 for Rust. Attackers can exhaust all memory via Vec::reserve calls. | Цифровой продукт используется в мультитенантном режиме (для каждого тенанта своя копия Цифрового продукта), что, в случае реализации уязвимости, отразится только на одном тенанте. Работа Цифрового продукта на постоянной основе подвергается мониторингу со стороны дежурной службы Цифрового продукта, что позволяет отреагировать на возможную атаку с использованием данной уязвимости. Цифровой продукт будет перезапущен без потери данных | Уязвимость компенсируется |

Анализ полученных результатов показал, что для пакетов **Hadoop 3.1.3**
и **HBASE 2.2.3** эксплуатируемых уязвимостей, с учетом приведенных компенсационных мер, не выявлено.

**Вывод**: в результате анализа по открытым источникам в ОО эксплуатируемые (не компенсированные) уязвимости **не выявлены**.

## 7.3. Анализ отсутствия идентифицированных уязвимостей при проведении тестирования проникновения

### 7.3.1. Проведение тестирования проникновения идентифицированных уязвимостей

Тестирование проникновения для ОО не проводилось, так как идентифицированных эксплуатируемых уязвимостей в ходе анализа документации на ОО и анализа отсутствия потенциальных уязвимостей в ОО, полученных при поиске информации в общедоступных источниках, выявлено не было.

### 7.3.2. Результаты тестирования проникновения идентифицированных уязвимостей

Тестирование проникновения для ОО не проводилось.

**Вывод:** в связи с отсутствием выявленных идентифицированных эксплуатируемых уязвимостей для ОО, данное исследование не проводится.

**Заключение**

На основании результатов проведенных испытаний можно сделать вывод, что в [наименование цифрового продукта], при выполнении выше описанных компенсирующих мер, применимых для него уязвимостей, **не выявлено**. Цифровой продукт функционирует в безопасном режиме работы.

1. В качестве примера в настоящем документе в качестве модулей цифрового продукта, используется следующее ПО]:

	* Apache HBase 2.2.3
	* Apache Hadoop 3.1 [↑](#footnote-ref-2)