# Курсовая работа "Защищённый контур" (Профессия Специалист по информационной безопасности)

## Легенда

Компания Х использует корпоративное сетевое приложение "Защищённый контур", позволяющее "безопасно" обмениваться корпоративной информацией (в том числе хранить персональные данные клиентов и информацию, отнесённую к коммерческой тайне). Вам предстоит проанализировать само приложение на уязвимости, а также настройки ОС на серверах, где это приложение функционирует.

Компания разработчик поставляет уже настроенный сервер в виде [OVA](https://drive.google.com/file/d/16uICxKQN91ZqjGa5a9AGml_WqG4oVXzp/view?usp=sharing) (md5 = 5935192d257a003b85584a84dec83367), который (по их заверениям) вполне безопасен и может использоваться "из коробки" (т.е. достаточно импортировать в среду виртуализации и можно запускать в боевой среде).

По информации, полученной от разработчика, цитата: "приложение содержит механизмы безопасности и может использоваться при построении ИСПД до 4 УЗ включительно и систем, обрабатывающих коммерческую тайну".

Документация на приложение разработчиком не предоставлена, поскольку, цитата: "интерфейс интуитивно понятный, обучающих материалов для пользователей не требуется".

Исходные коды так же не предоставлены.

Вас, как специалиста, попросили выполнить анализ данного приложения с точки зрения его реальной защищённости.

Исходное описание задания: <https://github.com/netology-code/sib-secure-kontur-diploma>

## Задание:

Подготовьте отчёт о:

1. Найденных несоответствиях системы требованиям нормативных документов\*
2. Найденных "слабостях" (которые могут привести к уязвимостям) и предложение по необходимым мерам для их устранения (если такие меры возможно принять).

Формат отчёта - свободный, но обязательно должен включать указанные выше два пункта.

Примечание\*: в части документов нужно:

1. ПДн: реализация мер по обеспечению безопасности в части ИАФ, УПД
2. КТ: "разрешение или запрет доступа к информации, составляющей коммерческую тайну" посредством механизмов разграничения доступа, встроенных в приложение (механизмы ОС и сторонних сервисов рассматривать не нужно)

## Решение:

1. **Найденных несоответствиях системы требованиям нормативных документов**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Уровни защищенности персональных данных | | |
| 4 | Оценка системы ЗК | Комментарий |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | |  |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | - | Не обеспечивается, нет разграничения по правам, любой может сразу добавлять или удалять данные |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | - | Не обеспечивается что позволит подбирать логины и пароли методами перебора |
| V. Регистрация событий безопасности (РСБ) | | | |  |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | - | Не обеспечивается |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | - | Не обеспечивается |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | - | Не обеспечивается |
| РСБ.7 | Защита информации о событиях безопасности | + | - | Не обеспечивается |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | |  |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | - | Не обеспечивается, версия системы не указана |

1. **Найденные "слабости" (которые могут привести к уязвимостям) и предложение по необходимым мерам для их устранения (если такие меры возможно принять).**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Код | Комментарий | Название | Балл | Название ру | Описание ру |
| **2** | [CWE-79](https://cwe.mitre.org/data/definitions/79.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 45.97 | CWE-79: неправильная нейтрализация ввода во время генерации веб-страницы ("Межсайтовый скриптинг") | Программное обеспечение не нейтрализует или неправильно нейтрализует контролируемый пользователем ввод перед его помещением в выходные данные, которые используются в качестве веб-страницы, которая предоставляется другим пользователям. |
| **3** | [CWE-89](https://cwe.mitre.org/data/definitions/89.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22.11 | CWE-89: Неправильная нейтрализация специальных элементов, используемых в команде SQL ("SQL-инъекция") | Программное обеспечение создает всю или часть команды SQL, используя внешние входные данные от вышестоящего компонента, но оно не нейтрализует или неправильно нейтрализует специальные элементы, которые могут изменить предполагаемую команду SQL, когда она отправляется нижестоящему компоненту. |
| **4** | [CWE-20](https://cwe.mitre.org/data/definitions/20.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Input Validation | 20.63 | CWE-20: Неправильная проверка входных данных | Продукт получает входные данные или данные, но не проверяет или неправильно проверяет, что входные данные обладают свойствами, необходимыми для безопасной и правильной обработки данных. |
| **10** | [CWE-434](https://cwe.mitre.org/data/definitions/434.html) | Позволяет любые файлы сохранять | Unrestricted Upload of File with Dangerous Type | 9.56 | CWE-434: неограниченная загрузка файла с опасным типом | Программное обеспечение позволяет злоумышленнику загружать или передавать файлы опасных типов, которые могут быть автоматически обработаны в среде продукта. |

1. **КТ: "разрешение или запрет доступа к информации, составляющей коммерческую тайну" посредством механизмов разграничения доступа, встроенных в приложение (механизмы ОС и сторонних сервисов рассматривать не нужно)**

Не обеспечивается механизм разграничения доступа на уровне документов и прав работы с документами: создание, изменение, удаление, в привязке к конкретным пользователям.

1. **Предложения**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Несоответствие | Слабость | Меры по устранению |
| 1 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |  | Управления правами для пользователя (создание, изменение, удаление) |
| 2 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |  | Ограничение на вход и блокировка пользователя |
| 3 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |  | Введение системы логирования действий пользователей |
| 4 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |  | Введение системы логирования действий пользователей |
| 5 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |  | Введение системы логирования действий пользователей |
| 6 | Защита информации о событиях безопасности |  | Введение системы логирования действий пользователей |
| 7 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |  | Создание системы установки обновлений и версий |
| 8 |  | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Доработка приложения и добавление фильтрации при вводе и сохранении информации |
| 9 |  | Позволяет любые файлы сохранять | Доработка приложения добавления ограничений на типы сохраняемых файлов |
| 10 |  | Не обеспечивается механизм разграничения доступа на уровне документов и прав работы с документами: создание, изменение, удаление, в привязке к конкретным пользователям. | Разработка механизма разграничения доступа на уровне документов и прав работы с документами: создание, изменение, удаление, в привязке к конкретным пользователям. |

**Приложение 1**

**Полный отчет по всем пунктам:**

Оценка системы на соответствие приказу по персональным данным:

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ

от 18 февраля 2013 г. N 21

СОСТАВ И СОДЕРЖАНИЕ

МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,

НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ

ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Уровни защищенности персональных данных | | |
| 4 | Оценка системы ЗК | Комментарий |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | |  |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | Производится по логину и паролю |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | Производится администраторами |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | Обеспечивается |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | Обеспечивается |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | Не предусмотрено |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | |  |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | Обеспечивается |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | Реализован ролевой метод |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | Обеспечивается |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | Обеспечено |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | - | Не обеспечивается, нет разграничения по правам, любой может сразу добавлять или удалять данные |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | - | Не обеспечивается что позволит подбирать логины и пароли методами перебора |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | - | Не предусмотрено |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | - | Не предусмотрено |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | - | Не предусмотрено |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | - | Не предусмотрено |
| V. Регистрация событий безопасности (РСБ) | | | |  |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | - | Не обеспечивается |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | - | Не обеспечивается |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | - | Не обеспечивается |
| РСБ.7 | Защита информации о событиях безопасности | + | - | Не обеспечивается |
| VI. Антивирусная защита (АВЗ) | | | |  |
| АВЗ.1 | Реализация антивирусной защиты | + | - | Не обеспечивается |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | - | Не обеспечивается |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | |  |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | - | Не обеспечивается, версия системы не указана |
| XI. Защита среды виртуализации (ЗСВ) | | | |  |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | - | Не предусмотрено |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | - | Не предусмотрено |
| XII. Защита технических средств (ЗТС) | | | |  |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + | - | Не предусмотрено |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | - | Не предусмотрено |
| XIII. Защита информационной системы, ее средств,  систем связи и передачи данных (3ИС) | | | |  |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | - | Не предусмотрено |

**2022 CWE Top 25 Most Dangerous Software Weaknesses**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Код | Комментарий | Описание | Балл | Название ру | Описание ру | Подробно ру | Связанные пункты |
| **1** | [CWE-787](https://cwe.mitre.org/data/definitions/787.html) | Программное | Out-of-bounds Write | 64.20 | CWE-787: запись за пределами | Программное обеспечение записывает данные после конца или до начала предполагаемого буфера. | Как правило, это может привести к повреждению данных, сбою или выполнению кода. Программное обеспечение может изменять индекс или выполнять арифметику указателей, которая ссылается на ячейку памяти, которая находится за пределами границ буфера. Затем последующая операция записи приводит к неопределенным или неожиданным результатам. | 119  121  122  123  124 |
| **2** | [CWE-79](https://cwe.mitre.org/data/definitions/79.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 45.97 | CWE-79: неправильная нейтрализация ввода во время генерации веб-страницы ("Межсайтовый скриптинг") | Программное обеспечение не нейтрализует или неправильно нейтрализует контролируемый пользователем ввод перед его помещением в выходные данные, которые используются в качестве веб-страницы, которая предоставляется другим пользователям. | Уязвимости межсайтового скриптинга (XSS) возникают, когда:  Ненадежные данные поступают в веб-приложение, как правило, из веб-запроса.  Веб-приложение динамически генерирует веб-страницу, содержащую эти ненадежные данные.  Во время генерации страницы приложение не препятствует тому, чтобы данные содержали контент, исполняемый веб-браузером, такой как JavaScript, HTML-теги, HTML-атрибуты, события мыши, Flash, ActiveX и т.д.  Жертва посещает созданную веб-страницу через веб-браузер, который содержит вредоносный скрипт, который был введен с использованием ненадежных данных.  Поскольку скрипт поступает с веб-страницы, отправленной веб-сервером, веб-браузер жертвы выполняет вредоносный скрипт в контексте домена веб-сервера.  Это фактически нарушает намерение политики веб-браузера того же происхождения, которая гласит, что скрипты в одном домене не должны иметь доступа к ресурсам или запускать код в другом домене. | 74  80  81  82  83  84  85  86  87 |
| **3** | [CWE-89](https://cwe.mitre.org/data/definitions/89.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 22.11 | CWE-89: Неправильная нейтрализация специальных элементов, используемых в команде SQL ("SQL-инъекция") | Программное обеспечение создает всю или часть команды SQL, используя внешние входные данные от вышестоящего компонента, но оно не нейтрализует или неправильно нейтрализует специальные элементы, которые могут изменить предполагаемую команду SQL, когда она отправляется нижестоящему компоненту. | Без достаточного удаления или цитирования синтаксиса SQL в управляемых пользователем входных данных сгенерированный SQL-запрос может привести к тому, что эти входные данные будут интерпретироваться как SQL вместо обычных пользовательских данных. Это может быть использовано для изменения логики запроса в обход проверок безопасности или для вставки дополнительных инструкций, которые изменяют серверную базу данных, возможно, включая выполнение системных команд.  Внедрение SQL-инъекций стало распространенной проблемой для веб-сайтов, управляемых базами данных. Недостаток легко обнаруживается и легко используется, и поэтому любой сайт или программный пакет даже с минимальной базой пользователей, вероятно, будет подвержен попытке атаки такого рода. Этот недостаток зависит от того факта, что SQL не делает реального различия между плоскостями управления и данными. | 943  564 |
| **4** | [CWE-20](https://cwe.mitre.org/data/definitions/20.html) | Допускается сохранение спецсимволов и можно сохранить какой нибудь сценарий при вводе | Improper Input Validation | 20.63 | CWE-20: Неправильная проверка входных данных | Продукт получает входные данные или данные, но не проверяет или неправильно проверяет, что входные данные обладают свойствами, необходимыми для безопасной и правильной обработки данных. | Проверка входных данных - это часто используемый метод проверки потенциально опасных входных данных, чтобы гарантировать, что входные данные безопасны для обработки в коде или при обмене данными с другими компонентами. Когда программное обеспечение не проверяет ввод должным образом, злоумышленник может обработать ввод в форме, которая не ожидается остальной частью приложения. Это приведет к тому, что части системы получат непреднамеренный ввод, что может привести к изменению потока управления, произвольному управлению ресурсом или выполнению произвольного кода.  Однако проверка входных данных - не единственный метод обработки входных данных. Другие методы пытаются преобразовать потенциально опасные входные данные во что-то безопасное, например, фильтрация (CWE-790), которая пытается удалить опасные входные данные, или кодирование / экранирование (CWE-116), которое пытается гарантировать, что входные данные не будут неверно истолкованы, когда они будут включены в выходные данные для другого компонента. Существуют и другие методы (дополнительные примеры см. в CWE-138). | Изображение выглядит как стол  Автоматически созданное описание |
| **5** | [CWE-125](https://cwe.mitre.org/data/definitions/125.html) | Программирование | Out-of-bounds Read | 17.67 | CWE-125: чтение за пределами | Программное обеспечение считывает данные после конца или до начала предполагаемого буфера. | Как правило, это может позволить злоумышленникам считывать конфиденциальную информацию из других ячеек памяти или вызывать сбой. Сбой может произойти, когда код считывает переменный объем данных и предполагает, что существует сигнализатор для остановки операции чтения, такой как NUL в строке. Ожидаемый сигнальный сигнал может отсутствовать в памяти вне пределов, что приводит к считыванию избыточных данных, что приводит к ошибке сегментации или переполнению буфера. Программное обеспечение может изменять индекс или выполнять арифметику указателей, которая ссылается на ячейку памяти, которая находится за пределами границ буфера. Последующая операция чтения приводит к неопределенным или неожиданным результатам. | 119  126  127 |
| **6** | [CWE-78](https://cwe.mitre.org/data/definitions/78.html) | Программирование | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 17.53 | CWE-78: неправильная нейтрализация специальных элементов, используемых в команде операционной системы ("Внедрение команды операционной системы") | Программное обеспечение полностью или частично создает команду операционной системы, используя входные данные, поступающие извне от вышестоящего компонента, но оно не нейтрализует или неправильно нейтрализует специальные элементы, которые могут изменить предполагаемую команду операционной системы, когда она отправляется нижестоящему компоненту. | Это может позволить злоумышленникам выполнять неожиданные, опасные команды непосредственно в операционной системе. Эта слабость может привести к уязвимости в средах, в которых злоумышленник не имеет прямого доступа к операционной системе, например, в веб-приложениях. С другой стороны, если уязвимость возникает в привилегированной программе, это может позволить злоумышленнику указывать команды, которые обычно недоступны, или вызывать альтернативные команды с привилегиями, которых у злоумышленника нет. Проблема усугубляется, если скомпрометированный процесс не следует принципу наименьших привилегий, поскольку команды, контролируемые злоумышленником, могут выполняться со специальными системными привилегиями, что увеличивает размер ущерба. | 77  88 |
| **7** | [CWE-416](https://cwe.mitre.org/data/definitions/416.html) | Программирование | Use After Free | 15.50 | CWE-416: использовать после освобождения | Обращение к памяти после ее освобождения может привести к сбою программы, использованию неожиданных значений или выполнению кода | Использование ранее освобожденной памяти может иметь любое количество неблагоприятных последствий, начиная от искажения достоверных данных и заканчивая выполнением произвольного кода, в зависимости от экземпляра и времени возникновения ошибки. Самый простой способ, которым может произойти повреждение данных, заключается в повторном использовании системой освобожденной памяти. Ошибки использования после освобождения имеют две общие и иногда перекрывающиеся причины:  Условия ошибки и другие исключительные обстоятельства.  Путаница в том, какая часть программы отвечает за освобождение памяти. | 825 |
| **8** | [CWE-22](https://cwe.mitre.org/data/definitions/22.html) | Нет | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 14.08 | CWE-22: неправильное ограничение пути к каталогу с ограниченным доступом ("Обход пути") | Программное обеспечение использует внешний ввод для создания имени пути, предназначенного для идентификации файла или каталога, расположенного под ограниченным родительским каталогом, но программное обеспечение не нейтрализует должным образом специальные элементы в имени пути, которые могут привести к разрешению имени пути к местоположению, находящемуся за пределами ограниченного каталога. |  | Изображение выглядит как стол  Автоматически созданное описание |
| **9** | [CWE-352](https://cwe.mitre.org/data/definitions/352.html) | Программирование | Cross-Site Request Forgery (CSRF) | 11.53 | CWE-352: подделка межсайтовых запросов (CSRF) | Веб-приложение не проверяет или не может в достаточной степени проверить, был ли правильно сформированный, действительный, согласованный запрос преднамеренно предоставлен пользователем, отправившим запрос. | Когда веб-сервер предназначен для получения запроса от клиента без какого-либо механизма проверки того, что он был отправлен намеренно, злоумышленник может обмануть клиента, заставив его сделать непреднамеренный запрос к веб-серверу, который будет рассматриваться как аутентичный запрос. Это может быть сделано с помощью URL, загрузки изображения, XMLHttpRequest и т.д. И может привести к раскрытию данных или непреднамеренному выполнению кода. |  |
| **10** | [CWE-434](https://cwe.mitre.org/data/definitions/434.html) | Позволяет любые файлы сохранять | Unrestricted Upload of File with Dangerous Type | 9.56 | CWE-434: неограниченная загрузка файла с опасным типом | Программное обеспечение позволяет злоумышленнику загружать или передавать файлы опасных типов, которые могут быть автоматически обработаны в среде продукта. | Термин "неограниченная загрузка файла" используется в базах данных уязвимостей и в других местах, но он недостаточно точен. Фраза может быть истолкована как отсутствие ограничений на размер или количество загружаемых файлов, что является проблемой потребления ресурсов. | Изображение выглядит как стол  Автоматически созданное описание |
| **11** | [CWE-476](https://cwe.mitre.org/data/definitions/476.html) | Программирование | NULL Pointer Dereference | 7.15 | CWE-476: разыменование нулевого указателя | Разыменование нулевого указателя происходит, когда приложение разыменовывает указатель, который, как ожидается, будет действительным, но имеет значение NULL, что обычно приводит к сбою или завершению работы. |  |  |
| **12** | [CWE-502](https://cwe.mitre.org/data/definitions/502.html) | Программирование | Deserialization of Untrusted Data | 6.68 | CWE-502: десериализация ненадежных данных | Приложение десериализует ненадежные данные без достаточной проверки того, что результирующие данные будут действительными. | Часто бывает удобно сериализовать объекты для обмена данными или сохранить их для последующего использования. Однако десериализованные данные или код часто могут быть изменены без использования предоставленных функций доступа, если они не используют криптографию для защиты. Кроме того, любая криптография все равно будет защищена на стороне клиента, что является опасным допущением безопасности.  Нельзя доверять тому, что ненадежные данные правильно сформированы.  Когда разработчики не накладывают ограничений на "цепочки гаджетов" или серии вызовов экземпляров и методов, которые могут выполняться самостоятельно во время процесса десериализации (т. Е. До того, как объект будет возвращен вызывающей стороне), злоумышленники иногда могут использовать их для выполнения несанкционированных действий, таких как создание оболочки. |  |
| **13** | [CWE-190](https://cwe.mitre.org/data/definitions/190.html) | Программирование | Integer Overflow or Wraparound | 6.53 | CWE-190: целочисленное переполнение или обтекание |  | Программное обеспечение выполняет вычисление, которое может привести к целочисленному переполнению или обтеканию, когда логика предполагает, что результирующее значение всегда будет больше исходного значения. Это может привести к другим недостаткам, когда вычисления используются для управления ресурсами или контроля выполнения. |  |
| **14** | [CWE-287](https://cwe.mitre.org/data/definitions/287.html) | Программирование | Improper Authentication | 6.35 | CWE-287: неправильная аутентификация | Когда субъект утверждает, что у него есть заданный идентификатор, программное обеспечение не доказывает или недостаточно доказывает, что утверждение верно. |  |  |
| **15** | [CWE-798](https://cwe.mitre.org/data/definitions/798.html) | Нет | Use of Hard-coded Credentials | 5.66 | CWE-798: использование жестко запрограммированных учетных данных | Программное обеспечение содержит жестко запрограммированные учетные данные, такие как пароль или криптографический ключ, которые оно использует для собственной входящей аутентификации, исходящей связи с внешними компонентами или шифрования внутренних данных. | Жестко запрограммированные учетные данные обычно создают значительную брешь, которая позволяет злоумышленнику обойти аутентификацию, настроенную администратором программного обеспечения. Системному администратору может быть трудно обнаружить этот пробел. Даже если это обнаружено, исправить это может быть сложно, поэтому администратор может быть вынужден полностью отключить продукт. Существует два основных варианта:  Входящие: программное обеспечение содержит механизм аутентификации, который проверяет входные учетные данные на соответствие жестко запрограммированному набору учетных данных.  Исходящие: программное обеспечение подключается к другой системе или компоненту и содержит жестко запрограммированные учетные данные для подключения к этому компоненту. | Изображение выглядит как стол  Автоматически созданное описание |
| **16** | [CWE-862](https://cwe.mitre.org/data/definitions/862.html) | Нет | Missing Authorization | 5.53 | CWE-862: отсутствует авторизация | Программное обеспечение не выполняет проверку авторизации, когда субъект пытается получить доступ к ресурсу или выполнить действие. | Предполагая, что пользователь имеет заданную личность, авторизация - это процесс определения, может ли этот пользователь получить доступ к данному ресурсу, на основе привилегий пользователя и любых разрешений или других спецификаций контроля доступа, которые применяются к ресурсу.  Когда проверки контроля доступа не применяются, пользователи могут получать доступ к данным или выполнять действия, которые им не следует разрешать выполнять. Это может привести к широкому кругу проблем, включая раскрытие информации, отказ в обслуживании и выполнение произвольного кода. | Изображение выглядит как стол  Автоматически созданное описание |
| **17** | [CWE-77](https://cwe.mitre.org/data/definitions/77.html) | Программирование | Improper Neutralization of Special Elements used in a Command ('Command Injection') | 5.42 | CWE-77: неправильная нейтрализация специальных элементов, используемых в команде ("Внедрение команды") | Программное обеспечение создает всю команду или ее часть, используя внешние входные данные от вышестоящего компонента, но оно не нейтрализует или неправильно нейтрализует специальные элементы, которые могут изменить предполагаемую команду, когда она отправляется нижестоящему компоненту. | Уязвимости, связанные с внедрением команды, обычно возникают, когда:  1. Данные поступают в приложение из ненадежного источника.  2. Данные являются частью строки, которая выполняется приложением как команда.  3. Выполняя команду, приложение предоставляет злоумышленнику привилегии или возможности, которых у злоумышленника в противном случае не было бы. | Изображение выглядит как стол  Автоматически созданное описание |
| **18** | [CWE-306](https://cwe.mitre.org/data/definitions/306.html) | Программирование | Missing Authentication for Critical Function | 5.15 | CWE-306: отсутствует аутентификация для критической функции |  | Программное обеспечение не выполняет никакой аутентификации для функциональности, которая требует доказуемой идентификации пользователя или потребляет значительное количество ресурсов. |  |
| **19** | [CWE-119](https://cwe.mitre.org/data/definitions/119.html) | Программирование | Improper Restriction of Operations within the Bounds of a Memory Buffer | 4.85 | CWE-119: неправильное ограничение операций в пределах буфера памяти | Программное обеспечение выполняет операции с буфером памяти, но оно может выполнять чтение или запись в ячейку памяти, которая находится за пределами предполагаемой границы буфера. | Некоторые языки допускают прямую адресацию ячеек памяти и автоматически не гарантируют, что эти местоположения действительны для буфера памяти, на который ссылаются. Это может привести к выполнению операций чтения или записи в ячейках памяти, которые могут быть связаны с другими переменными, структурами данных или внутренними данными программы.  В результате злоумышленник может выполнить произвольный код, изменить предполагаемый поток управления, прочитать конфиденциальную информацию или вызвать сбой системы. |  |
| **20** | [CWE-276](https://cwe.mitre.org/data/definitions/276.html) | Программирование | Incorrect Default Permissions | 4.84 | CWE-276: неправильные разрешения по умолчанию |  | Во время установки установленные права доступа к файлам устанавливаются таким образом, чтобы позволить любому пользователю изменять эти файлы. |  |
| **21** | [CWE-918](https://cwe.mitre.org/data/definitions/918.html) | Программирование | Server-Side Request Forgery (SSRF) | 4.27 | CWE-918: подделка запросов на стороне сервера (SSRF) | Веб-сервер получает URL-адрес или аналогичный запрос от вышестоящего компонента и извлекает содержимое этого URL-адреса, но это недостаточно гарантирует, что запрос отправляется ожидаемому адресату. | Предоставляя URL-адреса неожиданным хостам или портам, злоумышленники могут создать впечатление, что сервер отправляет запрос, возможно, в обход средств контроля доступа, таких как брандмауэры, которые не позволяют злоумышленникам напрямую обращаться к URL-адресам. Сервер можно использовать в качестве прокси-сервера для сканирования портов хостов во внутренних сетях, использовать другие URL-адреса, например, для доступа к документам в системе (с помощью file://), или использовать другие протоколы, такие как gopher:// или tftp://, которые могут обеспечить больший контроль надсодержимое запросов. |  |
| **22** | [CWE-362](https://cwe.mitre.org/data/definitions/362.html) | Программирование | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 3.57 | CWE-362: параллельное выполнение с использованием общего ресурса с неправильной синхронизацией ("Условие гонки") |  | Программа содержит кодовую последовательность, которая может выполняться одновременно с другим кодом, и кодовая последовательность требует временного эксклюзивного доступа к общему ресурсу, но существует временное окно синхронизации, в котором общий ресурс может быть изменен другой кодовой последовательностью, которая работает одновременно. |  |
| **23** | [CWE-400](https://cwe.mitre.org/data/definitions/400.html) | Программирование | Uncontrolled Resource Consumption | 3.56 | CWE-400: неконтролируемое потребление ресурсов |  | Программное обеспечение не контролирует должным образом распределение и обслуживание ограниченного ресурса, тем самым позволяя субъекту влиять на количество потребляемых ресурсов, что в конечном итоге приводит к исчерпанию доступных ресурсов. |  |
| **24** | [CWE-611](https://cwe.mitre.org/data/definitions/611.html) | Программирование | Improper Restriction of XML External Entity Reference | 3.38 | CWE-611: неправильное ограничение ссылки на внешнюю сущность XML | Программное обеспечение обрабатывает XML-документ, который может содержать объекты XML, с URI, которые разрешаются для документов за пределами предполагаемой сферы контроля, в результате чего продукт вставляет неправильные документы в свои выходные данные. | XML-документы необязательно содержат определение типа документа (DTD), которое, среди прочих функций, позволяет определять сущности XML. Можно определить сущность, предоставив строку подстановки в виде URI. Анализатор XML может получить доступ к содержимому этого URI и встроить это содержимое обратно в XML-документ для дальнейшей обработки.  Отправляя XML-файл, который определяет внешнюю сущность с помощью file:// URI, злоумышленник может заставить обрабатывающее приложение прочитать содержимое локального файла. Например, URI, такой как "file:///c:/winnt/win.ini", обозначает (в Windows) файл C:\Winnt\win.ini , или файл:///etc/passwd обозначает файл паролей в системах на базе Unix. Используя URI с другими схемами, такими как http://, злоумышленник может заставить приложение отправлять исходящие запросы на серверы, с которыми злоумышленник не может связаться напрямую, что может быть использовано для обхода ограничений брандмауэра или сокрытия источника атак, таких как сканирование портов. |  |
| **25** | [CWE-94](https://cwe.mitre.org/data/definitions/94.html) | Программирование | Improper Control of Generation of Code ('Code Injection') |  | CWE-94: Неправильный контроль генерации кода ("Внедрение кода") |  | Программное обеспечение создает весь или часть сегмента кода, используя входные данные, поступающие извне от вышестоящего компонента, но оно не нейтрализует или неправильно нейтрализует специальные элементы, которые могут изменять синтаксис или поведение предполагаемого сегмента кода. |  |