**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«Bot-Trek Secure Bank»**

**Версия 1.0**

**ОПИСАНИЕ РЕАЛИЗАЦИИ**

**СОДЕРЖАНИЕ**

[Аннотация 3](#_Toc395034820)

[1. Назначение ПО 3](#_Toc395034821)

[2. Программно-аппаратные среды функционирования ПО 3](#_Toc395034822)

[3. Общие принципы функционирования ПО 4](#_Toc395034823)

[4. Реализация ПО 5](#_Toc395034824)

[4.1. Структура ПО 5](#_Toc395034825)

[4.2. Состав ПО 5](#_Toc395034826)

[4.3. Функции частей ПО 5](#_Toc395034827)

[5. Взаимодействие ПО с автоматизированными системами 6](#_Toc395034828)

[5.1. Принципиальная схема взаимодействия ПО 6](#_Toc395034829)

[5.2. Структура взаимодействия 6](#_Toc395034830)

[5.3. Порядок взаимодействия 7](#_Toc395034831)

[5.4. Данные, передаваемые пользовательским модулем 7](#_Toc395034832)

[6. Обеспечение информационной безопасности 8](#_Toc395034833)

[6.1. Обеспечение конфиденциальности пользовательских данных 8](#_Toc395034834)

[6.2. Защита передаваемых данных 9](#_Toc395034835)

[6.3. Безопасность периметра АС заказчика 9](#_Toc395034836)

[6.4. Обеспечение доступности 9](#_Toc395034837)

# Аннотация

Настоящий документ содержит описание реализации программного обеспечения «Bot-Trek Secure Bank» версии 1.0 (далее – ПО).

# Назначение ПО

ПО обеспечивает на устройстве пользователя выполнение следующих защитных функций защищаемого веб-ресурса:

* детектирование несанкционированных изменений в страницах защищаемого веб-ресурса;
* детектирование удаленного подключения к конечному устройству пользователя с использованием протоколов удаленного рабочего стола (RDP, TeamViewer, VNC и т.п.);
* выявления признаков утечки учетных данных пользователя защищаемого веб-ресурса с использованием phishing/pharming-атак;
* детектирование иных признаков работы вредоносного программного обеспечения на конечном устройстве пользователя.

# Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

* Windows Internet Explorer версии 8.0 и выше
* Google Chrome версии 4.0 и выше
* Mozilla Firefox версии 3.5 и выше
* Apple Safari версии 4.0 и выше
* Opera версии 10.5 и выше
* iOS Safari версии 3.2 и выше
* Opera Mobile версии 11.0 и выше
* Google Chrome for Android версии 11.0 и выше
* Mozilla Firefox for Android версии 26.0 и выше
* Windows Internet Explorer Mobile версии 10.0 и выше

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

# Общие принципы функционирования ПО

На рисунке 1 изображены общие принципы функционирования ПО.



Рисунок . Общие принципы функционирования ПО.

ПО представляет из себя пользовательский модуль, реализованный на языке JavaScript. ПО загружается совместно со страницами защищаемого веб-ресурса. ПО производит сбор контрольных данных со страницы защищаемого веб-ресурса и устройства клиента, и отсылает их для дальнейшего анализа в автоматизированную систему (далее – АС) ООО «Группа АйБи» (далее – Group-IB). В случае выявления свидетельств о работе вредоносного ПО на устройстве пользователя или проведения phishing-/pharming-атак, АС Group-IB незамедлительно извещает об этом заказчика.

Внедрение ПО не требует внесения каких-либо изменений в инфраструктуру заказчика и в логику работы защищаемого веб-ресурса. ПО не требует инсталляции на устройстве пользователя и работает совершенно прозрачно для него.

# Реализация ПО

## 4.1. Структура ПО

Структура ПО представлена на рис.1.



Рисунок . Структура ПО

## 4.2. Состав ПО

ПО состоит из пользовательского модуля, который реализован на языке JavaScript. Модуль загружается на устройство пользователя совместно с защищаемым веб-ресурсом.

Пользовательский модуль предназначен для сбора контрольных данных, непосредственно в контексте страниц защищаемого веб-ресурса на устройстве пользователя, и их пересылки через сеть Интернет в АС Group-IB для последующей обработки и выявления признаков работы вредоносного программного обеспечения на устройстве пользователя.

Пользовательский модуль включает в себя:

* Систему сбора контрольной данных о структуре страницы защищаемого веб-ресурса;
* Систему сбора идентификационных данных пользователя на защищаемом веб-ресурсе;
* Систему защиты обмена данными с АС;
* Систему обмена данными с АС.

## 4.3. Функции частей ПО

* Система сбора контрольных данных о структуре страницы защищаемого веб-ресурса:
	+ Сбор данных о JavaScript-коде;
	+ Сбор данных об iframe;
	+ Сбор данных о формах.
* Система сбора идентификационных данных пользователя на защищаемом веб-ресурсе:
	+ Получение имени учетной записи пользователя на защищаемом веб-ресурсе из форм для ее ввода в целях идентификации пользователя на стороне АС заказчика.
* Система защиты обмена данными с АС:
	+ Шифрование идентификационных данных пользователя на публичном RSA-ключе заказчика;
	+ Шифрование контрольных данных.
* Система обмена данными с АС
	+ Посылка зашифрованных контрольных данных в АС;
	+ Периодическая посылка сигнальных данных о работе пользовательского модуля в АС.

# Взаимодействие ПО с автоматизированными системами

## 5.1. Принципиальная схема взаимодействия ПО

Принципиальная схема взаимодействия ПО с АС заказчика и Group-IB представлена на рис.2.



Рисунок 2. Принципиальная схема взаимодействия ПО с автоматизированными системами

## 5.2. Структура взаимодействия

Во взаимодействии участвуют следующие компоненты:

* Браузер на устройстве пользователя с загруженным пользовательским модулем в составе страницы защищаемого веб-ресурса;
* АС Group-IB;
* АС заказчика.

АС Group-IB состоит из следующих компонент:

* Серверная инфраструктура. Принимает, обрабатывает и анализирует контрольные данные, полученные от пользовательского модуля;
* Сервер управления. Служит для взаимодействия заказчика с АС Group-IB;
* АРМ администратора. Обеспечивает настройку и сопровождение АС.

АС заказчика состоит из следующих компонент:

* Совокупность веб-серверов и серверов приложений веб-ресурса;
* Модуль автоматизации. Использует API к АС Group-IB для автоматизации реагирования на выявленные подозрительные события. Необходимость разработки этого модуля и правила реагирования определяются заказчиком;
* АРМ оператора. Служит для ознакомления с подозрительными событиями и управления настройками выявления таких событий.

## 5.3. Порядок взаимодействия

* Пользовательский модуль загружается на устройство клиента совместно со страницами защищаемого веб-ресурса;
* Пользовательский модуль собирает контрольные данные со страницы веб-ресурса и посылает их для дальнейшего анализа в АС Group-IB;
* Веб-серверы заказчика отсылают заголовки запросов от пользователя в АС Group-IB для выявления случаев блокировки работы пользовательского модуля вредоносным программным обеспечением;
* Серверная инфраструктура АС Group-IB анализирует полученные данные от пользовательского модуля и АС заказчика на предмет наличия признаков вредоносных действий на устройстве пользователя;
* При выявлении таких признаков АС Group-IB незамедлительно оповещает заказчика по электронной форме;
* Заказчик через сайт сервера управления АС Group-IB имеет возможность получить детальную информацию о выявленном подозрительном событии с идентификационной информацией о пользователе и его устройстве;
* Заказчик через сайт сервера управления АС Group-IB имеет возможность дать обратную связь по выявленному событию, которая будет учтена в последующей обработке получаемых данных от пользовательского модуля;
* Оповещение о событиях, их детальная информация и обратная связь по ним так же возможна с использованием API к АС Group-IB.

## 5.4. Данные, передаваемые пользовательским модулем

Пользовательский модуль передает следующие контрольные данные с устройства пользователя:

* Данные о пользователе:
	+ результат применения алгоритма SHA1 к имени учетной записи пользователя;
	+ результат применения алгоритма RSA с публичным ключом заказчика к имени учетной записи клиента;
	+ характеристики движения курсором.
* Данные о странице защищаемого веб-ресурса:
	+ javascript-код, загружаемый на страницы веб-ресурса;
	+ структуру и атрибуты веб-форм, размещенных на страницах веб-ресурса;
	+ атрибуты следующих HTML-элементов: iframe, object, embed, applet.
* Данные о браузере, через который производится доступ на веб-ресурс:
	+ User-Agent, куда входят:
		- Браузер и его версия;
		- Операционная система и ее версия;
		- Разрядность операционной системы;
		- Название и модель устройства клиента.
	+ Accept-Encoding;
	+ Accept-Language;
	+ разрешение экрана;
	+ глубина цвета;
	+ доступность ActiveX;
	+ часовой пояс;
	+ шрифты браузера;
	+ плагины браузера;
	+ поддерживаемые языки;
	+ canvas-отпечаток.
* Данные об устройстве, если поддерживается Adobe Flash Player:
	+ архитектура процессора;
	+ операционная система;
	+ используемая версия и ее разрядность (32/64 бита) Adobe Flash Player;
	+ размеры экрана;
	+ наличие touch-экрана;
	+ язык;
	+ системные шрифты.

# Обеспечение информационной безопасности

## 6.1. Обеспечение конфиденциальности пользовательских данных

В АС Group-IB не передается пользовательская информация кроме обезличенного имени учетной записи пользователя. Имя учетной записи пользователя передается в виде:

* результата хеш-функции от имени учетной записи;
* и результата шифрования имени учетной записи с использованием публичного RSA-ключа заказчика.

Обе операции производятся непосредственно на устройстве пользователя.

Получаемая заказчиком информация о подозрительном событии содержит зашифрованное имя учетной записи. Используя соответствующий приватный RSA-ключ, только заказчик может получить исходное имя пользователя.

Таким образом, имя пользователя недоступно третьим лицам, в том числе Group-IB.

## 6.2. Защита передаваемых данных

Весь обмен информации между пользовательским модулем, АС Group-IB и АС заказчика производится по протоколу HTTPS.

Передаваемые данные из пользовательского модуля в АС Group-IB дополнительно кодируются в целях защиты от вредоносного программного обеспечения, функционирующего на устройстве пользователя.

## 6.3. Безопасность периметра АС заказчика

Обмен между АС заказчика и АС Group-IB всегда инициируется только со стороны заказчика на следующие домены:

* <https://vojs.group-ib.ru>;
* <https://vobe.group-ib.ru>;
* <https://vo.group-ib.ru>.

Для защиты периметра заказчика может быть применен любой тип фильтрации, ограничивающий обмен между АС заказчика и указанными сайтами АС Group-IB. Необходимо отметить, что любому из вышеуказанных доменных имен соответствует несколько IP-адресов, которые используются для обеспечения отказоустойчивости и распределения нагрузки.

## 6.4. Обеспечение доступности

Недоступность АС Group-IB никак не отражается на доступности и работоспособности защищаемого веб-ресурса как на стороне пользователя, так и на стороне заказчика.

Тем не менее, АС Group-IB обеспечивает отказоустойчивость своей инфраструктуры.