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

**Версия 1.0**

**РУКОВОДСТВО АДМИНИСТРАТОРА**

**СОДЕРЖАНИЕ**

[Аннотация 3](#_Toc402217859)

[1. Назначение ПО 3](#_Toc402217860)

[2. Программно-аппаратные среды функционирования ПО 3](#_Toc402217861)

[3. Общие принципы функционирования ПО 4](#_Toc402217862)

[4. Обязанности и функции администратора заказчика 4](#_Toc402217863)

[5. Порядок встраивания 4](#_Toc402217864)

[5.1. Выбор схемы встраивания в инфраструктуру 5](#_Toc402217865)

[5.2. Выработка RSA-ключей 6](#_Toc402217866)

[5.3. Создание тестовых учетных записей 7](#_Toc402217867)

[5.4. Определение IP-подсетей заказчика, используемые при взаимодействии с АС Group-IB 7](#_Toc402217868)

[5.5. Передача регистрационных данных заказчика в Group-IB 8](#_Toc402217869)

[5.6. Получение настроенного пользовательского модуля 8](#_Toc402217870)

[5.7. Конфигурация веб-серверов заказчика 8](#_Toc402217871)

[5.7.1. Конфигурирование веб-сервера NGINX 9](#_Toc402217872)

[5.7.2. Конфигурирование веб-сервера Apache 9](#_Toc402217873)

[5.7.3. Конфигурирование веб-сервера Microsoft IIS 10](#_Toc402217874)

[5.8. Вставка ссылки на пользовательский модуль в страницы защищаемого веб-ресурса 10](#_Toc402217875)

[6. Поддержание функционирования ПО 10](#_Toc402217876)

[Приложение 1. Файл groupib-feedback.php 11](#_Toc402217877)

# Аннотация

Настоящий документ содержит руководство администратора по встраиванию программного обеспечения «Bot-Trek Secure Bank» версии 1.0 (далее – ПО) в защищаемый веб-ресурс.

# Назначение ПО

ПО обеспечивает выполнение следующих защитных функций на конечном устройстве пользователя 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.

Описание реализации ПО представлено в документе «Описание реализации».

# 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 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.

Детальная информация о реализации ПО представлена в руководстве «Описание реализации».

# Обязанности и функции администратора заказчика

В обязанности администратора входит следующее:

* Произвести встраивание ПО в защищаемый веб-ресурс
* Поддерживать функционирование ПО

# Порядок встраивания

Для встраивания ПО в защищаемый веб-ресурс необходимо выполнить следующие шаги:

* Выбрать схему встраивания в инфраструктуру;
* Выработать приватный и публичный RSA-ключи;
* Создать две тестовые учетные записи на защищаемом веб-ресурсе;
* Определить перечень IP-подсетей заказчика, которые будут использоваться при взаимодействии с АС ООО «Группа АйБи» (далее Group-IB);
* Передать полученные ранее регистрационные данные заказчика в Group-IB;
* Получить в ответ ссылку на настроенный под веб-ресурс пользовательский модуль;
* Сконфигурировать веб-серверы заказчика на дублирование заголовков HTTP-запросов от пользователя на адрес https://vo.group-ib.ru;
* Вставить в каждую необходимую страницу защищаемого веб-ресурса ссылку на пользовательский модуль.

## 5.1. Выбор схемы встраивания в инфраструктуру

Существует три схемы встраивания ПО в инфраструктуру заказчика:

1. Загрузка клиентского модуля и передача контрольных данных происходит на домены \*.group-ib.ru;
2. IP-адресы серверов Group-IB регистрируются как домен следующего уровня в основной домен заказчика;
3. Загрузка клиентского модуля и передача контрольных данных производится через веб-серверы заказчика.

У каждой из схем есть свои достоинства и недостатки, оптимальное сочетание которых определяется заказчиком исходя из условий использования защищаемого веб-ресурса:

|  |  |  |
| --- | --- | --- |
| Схема | Достоинства | Недостатки |
| I | * Минимальные настройки на стороне заказчика;
* Отсутствие дополнительной нагрузки на ИТ-инфраструктуру заказчика;
* Быстрый вариант для пилотного использования ПО.
 | * На стороне браузера видны обращения на сторонние по отношению к заказчику ресурсы;
* Неработоспособность ПО при использовании дополнительных настроек политики или плагинов браузера, которые ограничивают обмен со сторонними веб-ресурсами по отношению к основному;
* Неработоспособность в IE6 и IE7, или в некоторых режимах обратной совместимости с более ранними версиями в IE8 и старше.
 |
| II | * Весь обмен между браузером пользователя и веб-ресурсом происходит с использованием доменов заказчика;
* Отсутствие блокировок работы клиентского модуля сторонним ПО;
* Средний уровень скрытности использования ПО для мошенника;
* Отсутствие дополнительной нагрузки на ИТ-инфраструктуру заказчика.
 | * В некоторых случаях требуется дополнительно выпускать ssl-сертификат на новые домены (описано ниже);
* Неработоспособность в IE6 и IE7, или в некоторых режимах обратной совместимости с более ранними версиями в IE8 и старше.
 |
| III | * Весь обмен между браузером пользователя и веб-ресурсом происходит с использованием его домена;
* Отсутствие блокировок работы клиентского модуля сторонним ПО;
* Высокий уровень скрытности использования ПО для мошенника;
* Работоспособность в IE6 и IE7, а также в режимах обратной совместимости с более ранними версиями в IE8 и старше.
 | * Требуются дополнительные настройки по трансляции запросов, относящихся к ПО, на web-серверах заказчика;
* Дополнительная нагрузка на инфраструктуру заказчика.
 |

В случае выбора схемы II, если действие ssl-сертификат защищаемого веб-ресурса не распространяется на домены следующего уровня, то необходимо выпустить отдельный ssl-сертификат на созданный домен.

Необходимые настройки в случае выбора схемы III будут предоставлены отдельно по запросу заказчика.

По выбору заказчика, незначительная часть серверной функциональности ПО генерации полиморфного клиентского модуля и его раздачи может быть передана заказчику. Это дает заказчику полный контроль над изменениями клиентского модуля и перечнем передаваемых данных с устройства пользователя. Инструкции по настройке вышеозначенного функционала будут предоставлены заказчику отдельно по запросу.

Далее указаны все общие шаги по внедрению ПО вне зависимости от выбранной схемы его внедрения.

## 5.2. Выработка RSA-ключей

Публичный RSA-ключ заказчика используется пользовательским модулем для шифрования имени учетной записи пользователя. Шифрование производится на устройстве пользователя. Зашифрованное имя учетной записи пользователя передается в АС Group-IB с другими контрольными деталями страницы защищаемого веб-ресурса.

Приватный RSA-ключ заказчика используется для расшифрования имени учетной записи пользователя при получении извещения из АС Group-IB о выявлении подозрительного события. Расшифрование производится на стороне заказчика. Таким образом, обеспечивается конфиденциальность пользовательских учетных данных.

Размерность ключей, срок действия и выбор программного обеспечения для выработки пары RSA-ключей определяется заказчиком.

Далее приведены команды для выработки ключей на примере свободного программного обеспечения OpenSSL ([www.openssl.org](http://www.openssl.org)):

1. Для создания приватного RSA-ключа необходимо выполнить команду:

openssl genrsa -out privkey.pem 1024

1. Для получения публичного RSA-ключа необходимо выполнить команду:

openssl rsa -pubout -in privkey.pem -out pubkey.pem

## 5.3. Создание тестовых учетных записей

Для настройки пользовательского модуля необходим доступ в защищаемый веб-ресурс. Для достоверной проверки, что пользовательский модуль не будет собирать контрольные данные, которые зависят от пользователя, необходимо использовать две различные учетные записи.

Условия предоставления тестовых учетных записей определяется заказчиком.

## 5.4. Определение IP-подсетей заказчика, используемые при взаимодействии с АС Group-IB

В целях обеспечения информационной безопасности, помимо использования протокола HTTPS при взаимодействии между компонентами АС заказчика и Group-IB, используется ограничение на публичные IP-адреса/подсети заказчика, с которых это взаимодействие возможно.

На рисунке 2 представлена принципиальная схема взаимодействия между АС заказчика и Group-IB:



Рисунок . Принципиальная схема взаимодействия между АС заказчика и Group-IB.

Необходимо определить все IP-адреса/подсети заказчика, которые будут участвовать в обмене между следующими компонентами АС:

* Веб-серверы АС заказчика и Серверной инфраструктурой АС Group-IB;
* Модуль автоматизации АС заказчика и Сервером управления АС Group-IB;
* АРМ оператора АС заказчика и Сервером управления АС Group-IB.

При определении IP-адресов/подсетей необходимо учесть существующие сценарии обеспечения непрерывности функционирования АС заказчика.

Политика ограничений по доступу к АС Group-IB со стороны компонент АС заказчика определяется заказчиком самостоятельно. При этом необходимо учитываться следующее:

* все взаимодействие с АС Group-IB инициируется со стороны компонент АС заказчика по протоколу HTTPS;
* доменным именам АС Group-IB соответствует несколько IP-адресов в целях обеспечения бесперебойности работы АС и распределения нагрузки на нее.

## 5.5. Передача регистрационных данных заказчика в Group-IB

Через портал защищенной электронной почты Group-IB (<https://smail.group-ib.ru>) необходимо отправить письмо с заголовком «Bot-Trek IB registration» со следующими сведениями:

* Публичный RSA-ключ заказчика. Передача приватного RSA-ключа строго запрещена и потребует выработки новой пары RSA-ключей;
* Две тестовых учетных записи с паролями к защищаемому веб-ресурсу;
* Публичные IP-адреса/подсети заказчика, которые участвуют в обмене с АС Group-IB.

Если портал защищенной электронный почты Group-IB используется в первый раз, то необходимо пройти процесс регистрации на портале.

## 5.6. Получение настроенного пользовательского модуля

Для настройки пользовательского модуля под защищаемый веб-ресурс потребуется некоторый период времени, который зависит от сложности веб-ресурса. Данный период согласовывается с заказчиком отдельно.

В ответ на исходное письмо заказчика с регистрационными данными, по окончании настройки пользовательского модуля, Group-IB вышлет ссылку на него через портал защищенной почты.

## 5.7. Конфигурация веб-серверов заказчика

Для определения вмешательства в работу клиентского модуля или его блокировки вредоносным программным обеспечением на устройстве пользователя, АС Group-IB необходимо получать сигнальные данные о работе пользователей непосредственно с веб-серверов АС заказчика. Для этого достаточно дублировать заголовки HTTP-запросов, приходящие от пользователя на веб-серверы АС заказчика, и пересылать их в серверную инфраструктуру АС Group-IB. При этом содержимое самих HTTP-запросов пересылать не надо, тем самым обеспечивая конфиденциальность пользователей веб-ресурса.

Ниже приводятся инструкции по организации вышеописанного дублирования HTTP-запросов для каждого из веб-серверов.

### 5.7.1. Конфигурирование веб-сервера NGINX

В секциях location, которые отвечают за выдачу страниц защищаемого веб-ресурса или работу в режиме reverse-proxy для него, необходимо прописать директиву:

location / {

 …

 **post\_action /feedbaсk\_to\_group\_ib;**
}

В соответствующую секцию server необходимо добавить следующее определение /feedbaсk\_to\_group\_ib:

**location** /**feedback\_to\_group\_ib {
 proxy\_pass** [**https://vobe.group-ib.ru/feedback.php;**](http://beta.group-ib.ru/test.php) **proxy\_pass\_request\_body off;
 proxy\_set\_header Content-Length 0;
 proxy\_set\_header Referer ‘’;
 internal;
}**

Данные директивы инструктируют NGINX пересылать заголовки HTTP-запросов от пользователей веб-ресурса в АС Group-IB. Данные внутри запросов при этом не пересылаются.

Недоступность серверной инфраструктуры АС Group-IB никак не влияет на работоспособность АС заказчика.

### 5.7.2. Конфигурирование веб-сервера Apache

Для отправки сигнальных данных о работе пользователей непосредственно с веб-серверов АС заказчика используется стандартный модуль mod\_log\_config веб-сервера Apache. Необходимо удостовериться, что в конфигурационном файле веб-сервера указанный модуль загружается и активен.

В общей или в секции конфигурационного файла, отвечающего за сайт защищаемого веб-ресурса, необходимо задать перечень сигнальных данных для отправки в АС Group-IB:

**LogFormat "%{%Y-%m-%d %H:%M:%S %z}t|^|%a|^|%v|^|%U|^|%q|^|%{User-Agent}i|^|%{Cookie}i" groupib**

В секциях, отвечающих за отдачу ресурсов защищаемого веб-ресурса клиентам и прием запросов от них, необходимо указать следующую директиву:

**CustomLog "|/path/to/groupib-feedback.php" groupib**

ВНИМАНИЕ: Для снижения нагрузки как на веб-сервер заказчика, так и АС Group-IB имеет смысл последнюю директиву задавать только для основных ресурсов, таких как основные html-страницы, и исключить для второстепенных ресурсов сайта, таких как картинки, вспомогательные скрипты и т.п. При этом можно указанную выше директиву указывать на все секции, которые являются точками обработки запросов от браузера пользователя.

Содержимое файла groupib-feedback.php приведено в Приложении 1.

ВНИМАНИЕ: Важно, чтобы скрипт groupib-feedback.php был запускаемым.

### 5.7.3. Конфигурирование веб-сервера Microsoft IIS

## 5.8. Вставка ссылки на пользовательский модуль в страницы защищаемого веб-ресурса

Пользовательский модуль написан на языке JavaScript. Для его использования необходимо вставить в раздел HEAD необходимых HTML-страниц веб-ресурса следующую директиву:

**<script type=”text/javascript” src=[ссылка на пользовательский модуль]></script>**

ВНИМАНИЕ: указанная директива должна находиться сразу за <HEAD>.

# Поддержание функционирования ПО

Поддержание функционирования ПО состоит в контроле действия настроек, произведенных в рамках встраивания ПО. Иных регламентных мероприятий со стороны администратора заказчика ПО не требует.

# Приложение 1. Файл groupib-feedback.php

ВНИМАНИЕ: Важно, чтобы нижеприведенный скрипт имел атрибуты исполняемого файла.

**#!/usr/bin/php**

**<?php**

**# url for feedback requests**

**define("FEEDBACK\_URL", "**[**https://vobe.group-ib.ru/feedback-apache.php**](https://vobe.group-ib.ru/feedback-apache.php)**");**

**# parce CustomLog format**

**$param = preg\_split("@\|\^\|@", stream\_get\_line(STDIN, 1024, PHP\_EOL));**

**$object = (object) [**

**"time" => $param[0],**

**"ip" => $param[1],**

**"domain" => $param[2],**

**"url" => $param[3],**

**"args" => $param[4],**

**"user-agent" => $param[5],**

**"cookie" => $param[6]**

**];**

**# send params in post body (json)**

**$options = array(**

**'http' => array(**

**'header'  => "Content-type: application/json\r\n",**

**'method'  => 'POST',**

**'content' => json\_encode($object)**

**)**

**);**

**$context  = stream\_context\_create($options);**

**@file\_get\_contents(FEEDBACK\_URL, false, $context);**