**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ  
«Bot-Trek Intelligence»**

**Версия 1.0**

**ОПИСАНИЕ РЕАЛИЗАЦИИ**

**СОДЕРЖАНИЕ**

[1. Аннотация 3](#_Toc460504816)

[2. Назначение ПО 3](#_Toc460504817)

[3. Программно-аппаратные среды функционирования ПО 3](#_Toc460504818)

[4. Общие принципы функционирования ПО 4](#_Toc460504819)

[5. Реализация ПО 5](#_Toc460504820)

[5.1. Модуль регистрации инцидентов компрометации учетных данных 5](#_Toc460504821)

[5.2. Модуль оповещения о случаях выявления компрометации информации 7](#_Toc460504822)

[5.3. Модуль предоставления статистики и отчетности 7](#_Toc460504823)

[5.4. Модуль защиты удаленного доступа и контроля изменений 8](#_Toc460504824)

[6. Взаимодействие ПО с автоматизированными системами 9](#_Toc460504825)

[6.1. Авторизация 9](#_Toc460504826)

[6.2. Получение данных 10](#_Toc460504827)

# Аннотация

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

# Назначение ПО

Система учета скомпрометированной информации предназначена для сбора информации о случаях компрометации учетной информации пользователей информационных систем, компрометации информации о банковских картах, сбора информации о первичных получателях похищаемых денежных средств (далее - дропов), а так же предоставления интерфейса для отображения данных и оповещения о выявленных случаях компрометации данных с целью минимизации рисков мошенничества в отношении финансовых организаций в разных странах.

Основными целями создания Системы являются:

* Предоставление единого интерфейса регистрации фактов компрометации учетных данных пользователей интерактивных информационных систем (дистанционного банковского обслуживания, платежных систем, систем обмена электронными сообщениями, систем хранения данных в сети интернет и прочих электронных интерактивных систем);
* Консолидация разрозненной информации по компрометации информации в сферах финансового обслуживания, хранения данных, оказания государственных услуг и электронной коммерции;
* Генерация правил для систем предотвращения мошеннических операций, используемых организациями, участниками системы;
* Оперативное оповещение участников системы;
* Снижение уровня преступлений в сфере электронной коммерции;
* Ускорение процесс обмена информацией о мошенничестве между банками;
* Повышение качества и количества раскрываемых преступлений;
* Предоставление прозрачной статистической и аналитической информации

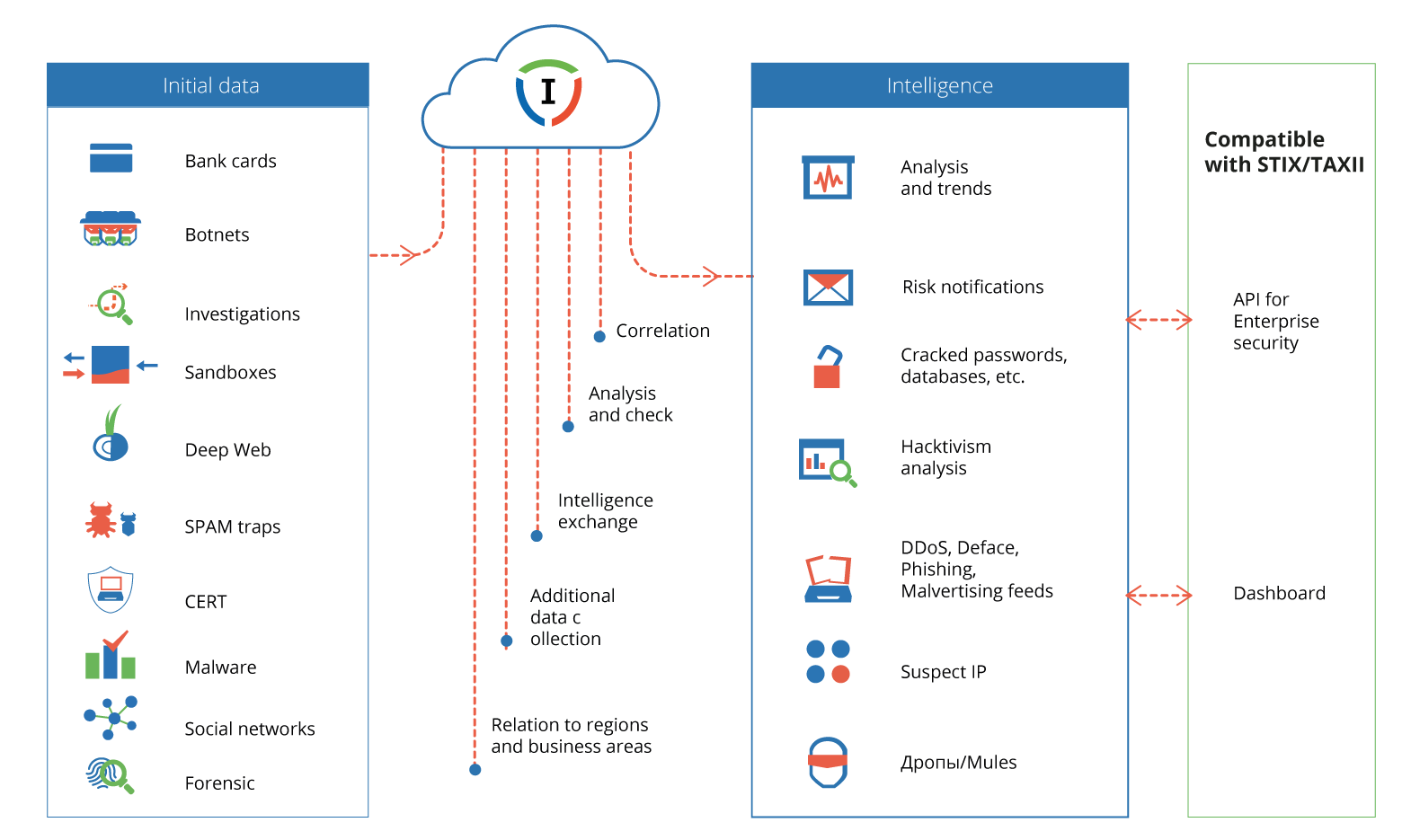
# Программно-аппаратные среды функционирования ПО

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

# Общие принципы функционирования ПО

Для сбора данных мы постоянно исследуем бот-сети различного назначения, вредоносные программы, которые были найдены в результате реагирования на самые опасные инциденты, присутствуем на самых закрытых хакерских форумах и собираем данные о новых трендах, угрозах, утечках. Все эти данные коррелируются между собой и переносятся в соответствующий раздел пользовательского интерфейса Bot-Trek Intelligence.



# Реализация ПО

Системы состоит из следующих модулей:

* Модуль регистрации инцидентов компрометации учетных данных
* Модуль оповещения о случаях выявления компрометации информации
* Модуль предоставления статистики и отчетности
* Модуль защиты удаленного доступа и контроля изменений

В рамках предоставляемого интерфейса операторы системы (сотрудники Group-IB) имеют возможность зарегистрировать выявленный факт компрометации учетных данных пользователей систем ДБО, иных учетных данных интерактивных интернет-сервисов, информации о банковской карте и сведений о дропах. Зачастую кроме самого факта компрометации Group-IB обладает дополнительными сведениями, полученными в результате работ внутренних информационных систем, такими как: IP-адрес скомпрометированного пользователя, точное время компрометации сведений, идентификатор копии установленного вредоносного ПО, идентификатор командного центра бот-сети, источник проведения мошенничества. Разработанный интерфейс предоставляет возможность внести максимально полную информацию о выявленном инциденте.

# Модуль регистрации инцидентов компрометации учетных данных

* доступ к подсистеме регистрации предоставляется через Веб-интерфейс;
* интерфейс обеспечивеаь обязательные и необязательные поля для заполнения (список полей приведен ниже);
* Поддержка стандартного формата импорта данных CSV – comma separated value, подразумевающая разделение полей данных стандартным разделителем, с возможностью указания разделителя в диалоге импорта данных;
* Поддержка корректного импортирования даты и времени инцидента из формата unix timestamp;
* Автоматическая ассоциация импортируемых данных с определенной организацией, в соответствии с настройками системы, по следующим идентификаторам:
  + Для аккаунтов систем ДБО и других интерактивных сервисов – по доменному имени
  + Для банковских карт - по унифицированному международному идентификатору BIN
  + Для дропов – по банковскому идентификатору, в зависимости от региона: БИК, SWIFT или RTN номера
* Автоматическое раскодирование импортируемых данных из стандартного способа кодирования POST-запросов
* Автоматическое определение региона скомпрометированного пользователя по IP-адресу в соответствии с geolocation-базой
* Автоматическое определение страны происхождения скомпрометированной карты по идентификатору BIN в соответствии с мировой базой BIN-идентификаторов.
* Корректное импортирование бинарных данных (изображения экрана, сертификаты, ключи доступа) с указанием ассоциированного банка в диалоге загрузки данных
* Обеспечение целостности и недублирования хранимых данных, с обеспечением уникальности ключевых полей в соответствии с используемой схемой базы данных
* Возможность указания произвольной даты выявления скомпрометированных данных с подстановкой текущей даты в случае незаполнения соответствующего поля.

В рамках предоставления интерфейса для регистрации инцидентов компрометации учетных данных пользователей систем ДБО и иных интерактивных сервисов, обязательной для заполнения должна быть следующая информация:

* Доменное имя либо ip-адрес на котором развернута система;
* идентификатор пользователя;
* IP-адрес;
* дата и время инцидента.

Следующая информация является необязательной для заполнения, однако интерфейс предусматривает данные поля:

* пароль пользователя;
* коды подтверждения операций;
* идентификатор копии вредоносного ПО;
* телефон;
* имя компьютера пользователя

В рамках предоставления интерфейса для регистрации информации о скомпрометированных банковских картах обязательной для заполнения должна быть следующая информация:

* номер карты;
* дата истечения карты;
* имя владельца;
* название банка;
* регион работы банка.

Следующая информация является необязательной для заполнения, однако интерфейс предусматривает данные поля:

* адрес владельца карты;
* телефонный номер;
* город;
* номер социального страхования;
* иная скомпрометированная информация.

# Модуль оповещения о случаях выявления компрометации информации

Созданные отчеты по фактам выявления компрометации данных с целью предотвращения мошенничества в режиме реального времени отправляются участникам Системы. Оперативное оповещение позволяет предотвратить мошеннические операции, что в значительной степени снижает количество успешных случаев мошенничества, повышает лояльность клиентов в сферах финансово-кредитного обслуживания и электронной коммерции.

* при регистрации в системе инцидентов компрометации данных происходит оповещение в режиме реального времени;
* оповещение приходит по электронной почте на адреса, указанные в настройках участника Системы, в отношении пользователей которого зафиксирован инцидент компрометации данных;

Оповещение по электронной почте содержит в себе как минимум следующую обязательную информацию:

* Тип выявленных данных
* Количество выявленных данных;
* Название организации.

Помимо уведомления в адрес участника Системы, в копию уведомления ставится ответственный сотрудник Group-IB для отслеживания работы системы уведомления и дополнительного учета выявляемых данных.

# Модуль предоставления статистики и отчетности

Зарегистрированные данные позволят предоставлять аналитическую и статистическую информацию о структуре, количестве и региональном распределении случаев компрометации учетной информации. Аналитическая информация выводиться, прежде всего, на главной странице в виде краткой сводки по количеству, типам, региональному и временному распределению данных.

Статистическая информация позволяет отслеживать темпы роста/спада активности злоумышленников в этой сфере, а также различные распределения по регионам.

* количество зарегистрированных инцидентов: общее и с разбивкой по типам данных;
* количество инцидентов за определенные промежутки времени;
* общий объем хранимых в системе данных;
* распределение случаев компрометации данных по странам и городам;
* распределение случаев компрометации данных по времени с отображением структуры данных;
* обеспечивается быстрая генерация статистических показателей даже на больших объемах хранимых данных: время отображения статистических показателей.

# Модуль защиты удаленного доступа и контроля изменений

Модуль защита удалённого доступа обеспечивает:

* сохранение конфиденциальности и целостности передаваемой информации;
* возможность ограничения доступа к системе для всех адресов кроме указанного в настройках, причем ограничение должно работать на канальном уровне.
* неотключаемый протокол доступа в Систему для каждого участника Системы. Для контроля удачных/неудачных попыток авторизации в личном кабинете должна быть отображена история авторизации.
* неотключаемый протокол внесения изменений в Систему и выгрузки данных из системы:
  + загрузка новых данных;
  + изменение параметров пользователей Системы;
  + выгрузка данных в отдельный файл со скачиванием через клиентский браузер;
  + создание новых пользователей Системы;
  + выдача пользователю дополнительных прав.

# Взаимодействие ПО с автоматизированными системами

Bot-trek Intelligence API предоставляет программируемый интерфейс для чтения данных по запросу из системы. API предназначено для автоматизированного получения информации из системы Bot-Trek Intelligence и интерации с внутренними системами безопасности и противодействия мошенничеству.

Пользователи API получают возможность выгружать данные и индикаторы из всех разделов системы, к которым они имеют доступ. API использует RESTful протокол, а ответы предоставляются в формате JSON.

Базовый URL API: <https://bt.group-ib.com/>.

# Авторизация

Для авторизация должны использовать login и api\_key. Способы передачи:

* В заголовках X-Auth-Login и X-Auth-Key (предпочтительно)
* В виде параметров login и key в теле POST-запроса (допустимо)

Запрос должен содержать заголовок "Accept: application/json " для указания на тип ожидаемых данных.

Пример запроса:

**GET /?module=get&action=accs&limit=1000&last=0 HTTP/1.1**

**Host**: bt.group-ib.com

**Accept**: application/json

**X-Auth-Login**: test\_user

**X-Auth-Key**: test\_key

**Connection**: Keep-Alive

**Keep-Alive**: 30

Ответ сервера должен быть со статусом HTTP 200, тело должно содержать объект в формате JSON. Если это не так, значит произошла ошибка на ранних этапах обработки запроса. Поля объекта JSON из ответа на запрос:

| **Поле ответа** | **Описание** |
| --- | --- |
| status | Статус ответа API. Коды статусов совпадают с аналогичными по смыслу статусами HTTP. |
| data | Если поле status = 200, то возвращаются данные на запрос API. |
| error | Если поле status <> 200, то возвращает сообщение об ошибке. |
| edata | Если поле status <> 200, дополнительная техническая информация об ошибке. |

Поле **data** может содержать любые типы данных, кроме null. Например, true/false, число, строка, объект или массив.

# Получение данных

Полный URL запроса на получение данных: https://bt.group-ib.com/?module=get&action=<action>&last=<last>&limit=<limit>

Параметр <action> указывает на тип запрашиваемых данных. Варианты значений:

| **Значение параметра <action>** | **Описание** |
| --- | --- |
| accs | Сведения о скомпрометированных логинах и паролях |
| cards | Сведения о скомпрометированных банковских картах |
| imei | Идентификаторы зараженных мобильных устройств |
| mules | Сведения о мошеннических счетах (черный обнал) |
| phishing | Фишинговые ресурсы |
| ddos | DDoS атаки |
| hacktivism | Сведения о Хактивизме |
| sample | Сведения о вредоносных программах из раздела Targeted malware |

Параметр <last> указывает на позицию, относительно которой следует сделать новую выборку. В первом запросе следует указать 0. Каждый ответ содержит поле last, значение которого следует использовать в параметре <last>следующего запроса.

Необязательный параметр <limit> ограничивает размер выборки. Допустимый диапазон значений: от 1 до 1000. Значение по умолчанию - 100. Так как размер атрибута inject\_dump может достигать нескольких мегабайт, в запросах action=sample максимально допустимое значение параметра <limit> снижено до 20, а значение по умолчанию - 10.

Необходимо повторять запросы в цикле до тех пор, пока в ответе не будет получено то же значение <last>, которое было указано в запросе. Альтернативно можно проверять поле count, значение которого должно быть равно limitдо тех пор, пока не будут исчерпаны доступные данные.

Необходимо сохранять значения <last> между сессиями выгрузки данных, чтобы обеспечить возобновление с места, на котором остановилась предыдущая сессия.

Выборка захватывает любые объекты, созданные или изменённые после момента времени, определяемого значением last. Поэтому возможно повторное получение одного и того же объекта (повторяющийся id).

Если объекты были удалены, их id будут перечислены в поле del.

Данные разделов Hacktivism и Targeted malware поддерживают переводы на несколько языков, поэтому соответствующие запросы API должны содержать параметр <lang>, указывающий требуемый язык.

Допустимые значения:

2 — Русский

3 — Английский