



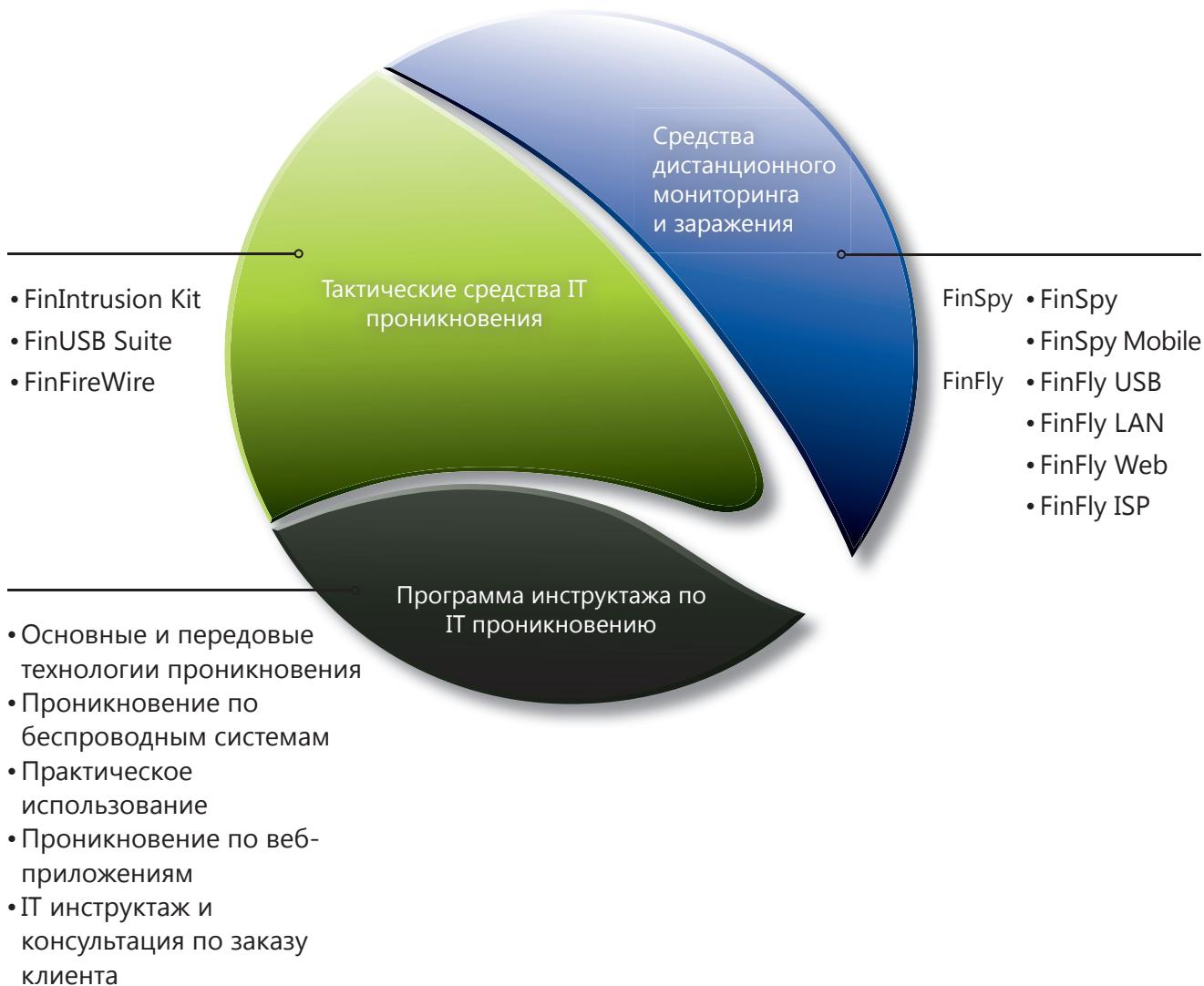
FINFISHER™ : ПРАВИТЕЛЬСТВЕННЫЕ ИТ ПРОНИКНОВЕНИЯ  
И СРЕДСТВА ДИСТАНЦИОННОГО  
МОНИТОРИНГА



**FINFISHER™**

[WWW.GAMMAGROUP.COM](http://WWW.GAMMAGROUP.COM)

IT INTRUSION

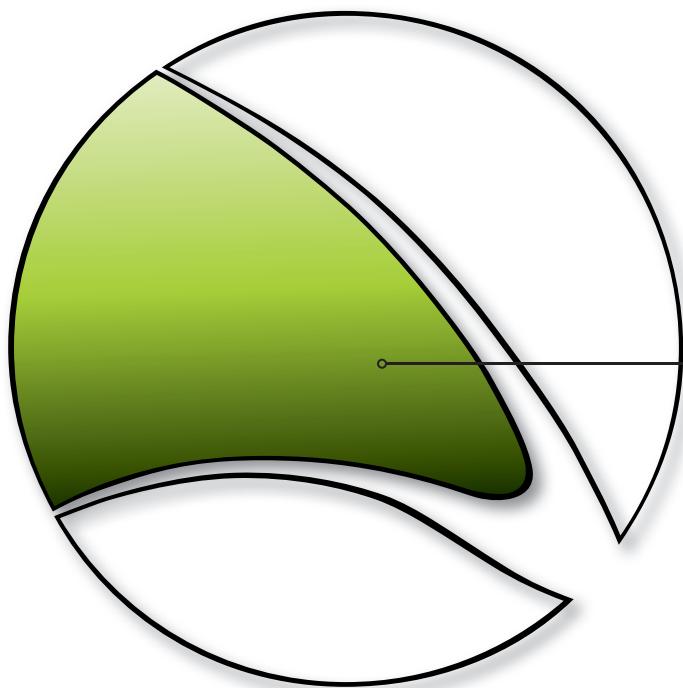


# Тактические средства IT проникновения

**FININTRUSION KIT**

**FINUSB SUITE**

**FINFIREWIRE**



Gamma решает вопросы в области IT проникновения с помощью средств, позволяющих повышать возможности наших клиентов. Простые в применении высококлассные средства и технологии дополняют ноу-хау разведывательных организаций, и позволяют им решать задачи проникновения на тактическом уровне.



**FINFISHER™**  
IT INTRUSION

# Тактические средства IT проникновения

## НАБОР FININTRUSION KIT

Набор «FinIntrusion Kit» спроектирован и разработан специалистами мирового класса по ИТ проникновению, имеющими более 10 лет опыта работы в данной сфере с различными группами экспертов (Tiger Teams/ Read Teams) по определению слабых сторон систем безопасности, как в частном, так и в правительственном секторе, оценивающих безопасность различных сетей и организаций.

Набор FinIntrusion Kit является результатом создания **современного и скрытого** операционного набора, который можно применять в наиболее распространенных **операциях ИТ проникновения** в оборонительных и наступательных сферах. Нашиими клиентами являются **Военные отделения по ведению войны в виртуальной среде, разведывательные организации, полицейские разведывательные отделы, и другие правоохранительные органы.**

### Пример применения 1: Команда технического наблюдения

Набор FinIntrusion Kit применялся при взломе **WPA шифрования** домашней беспроводной сети объекта и в последующем наблюдении за его **веб-почтой (Gmail, Yahoo, ...)** и **личными данными на сайтах интернет-сообществ (Facebook, MySpace, ...)**. Это позволило ведущим следствие осуществлять **дистанционный мониторинг** по этим учетным записям, находясь в своём штабе, без необходимости находиться в непосредственной близости с объектом.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	<b>Стратегические операции</b> <b>Тактические операции</b>
Возможности:	<b>Расшифровка WEP/WPA кодирования</b> <b>Мониторинг по сетям (включая SSL сессии)</b> <b>Атаки по ИТ проникновению</b>
Содержание:	<b>Аппаратное оборудование и программное обеспечение</b>

### Пример применения 2: ИТ безопасность

Некоторые клиенты применяли набор «FinIntrusion Kit» для успешного **нарушения системы безопасности** сетей и компьютерных систем в **наступательных и оборонительных** целях, используя при этом различные средства и технологии.

### Пример применения 3: Стратегические сценарии использования

Набор «FinIntrusionKit» широко применяется для того, чтобы получить дистанционный доступ к учетным записям электронной почты и веб-серверам объектов (напр. блогам, форумам) и наблюдать их действия, включая журналы регистрации запросов к доступу и многое другое.

### Обзор функций

- Обнаружение **беспроводных локальных сетей (802.11)** и работающих по **Bluetooth®** средств
- Восстановление WEP фраз-паролей (64 и 128 битов) **за 2-5 минут**
- **Взлом WPA1 и WPA2** фраз-паролей с помощью применения словарных атак
- Осуществление активного мониторинга по локальным сетям (проводным и беспроводным) и **извлечение имен пользователей и паролей даже с зашифрованных TLS/SSL сессий**
- Эмулирование **неавторизованных точек беспроводного доступа** (802.11)
- **Принудительное получение доступа к учетным записям электронной почты** в дистанционном режиме с помощью применения технологий проникновения, работающих по сетям, системам и паролям
- Проверка и **оценка безопасности сетей**

Пожалуйста,смотрите полный перечень функций в спецификации продукции.

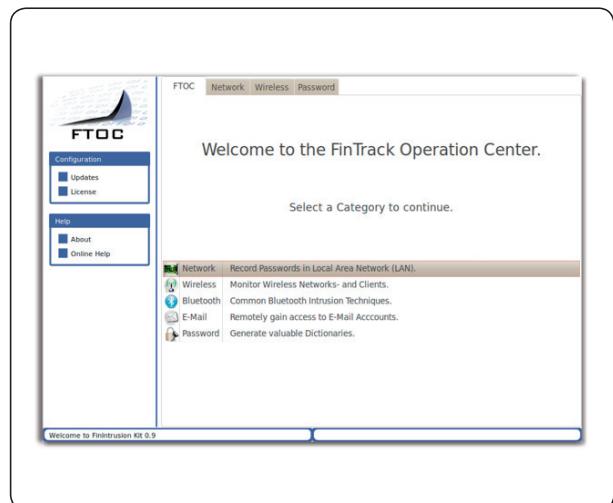


**FINFISHER™**  
IT INTRUSION

# Тактические средства IT проникновения

## НАБОР FININTRUSION KIT

### СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



#### FinIntrusion Kit – Скрытая Тактическая Система

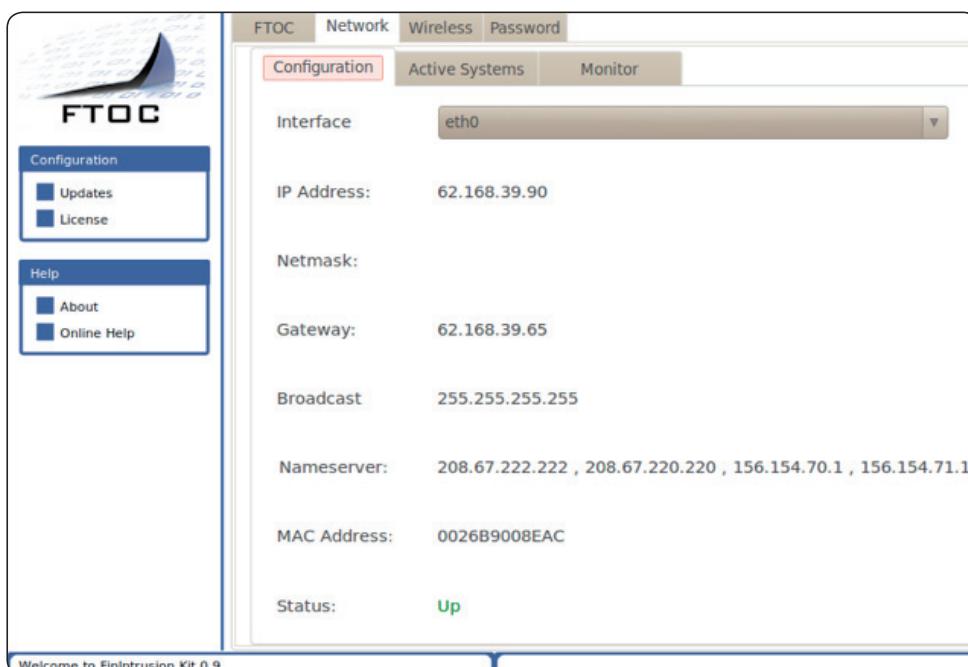
Основные составляющие IT проникновения:

- Адаптер высокой мощности WLAN
- Адаптер высокой мощности Bluetooth
- Антенны 802.11
- [USB диск для восстановления паролей]
- Прочие стандартные устройства IT проникновения

#### FinTrack Операционный Центр

- Графический интерфейс пользователя, позволяющий автоматические атаки IT проникновения

### Автоматизированный мониторинг в сетях LAN/WLAN



# Тактические средства IT проникновения

## НАБОР FININTRUSION KIT

### **СРЕДСТВО АКТИВНОГО ИЗВЛЕЧЕНИЯ ПАРОЛЕЙ В ПРОВОДНЫХ И БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ LAN/WLAN СЕТЯХ**

- Собирает даже SSL-зашифрованные данные, такие, как веб-почта, видео-порталы, банковские операции по Интернету, и многое другое

Main	Credentials		
Username	Password	Server	Protocol
dropbox	fr33dom	64.223.183.17	https
ftp	secret1	128.101.240.212	ftp
ftoc	password1	62.84.74.92	pop3

**Start**      **Delete**      **Save...**



# Тактические средства IT проникновения

## НАБОР FINUSB SUITE

Набор «FinUSB Suite» является многоцелевой продукцией, позволяющей правоохранительным и разведывательным организациям быстро и безопасно извлекать судебную информацию из компьютерных систем без необходимости привлекать обученных по ИТ операторов.

Данная система успешно применялась в операциях по всему миру и извлекла ценную разведывательную информацию о намеченных объектах при скрытых и открытых операциях.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	• Тактические операции
Возможности:	• Сбор информации Доступ к системам • Быстрое извлечение судебной информации
Содержание:	• Аппаратное оборудование и программное обеспечение

### Пример применения 1: Скрытая операция

Источнику информации в организованной преступной группировке (ОПГ) был вручен аппаратный ключ FinUSB, который скрыто извлекал данные учетной записи веб-серверов и электронной почты, и также документы Microsoft Office из систем объекта в то время как члены ОПГ использовали это USB-средство для **передачи обычных файлов**, таких, как музыка, видеозаписи и документы Office.

При получении данного USB-средства в штабе, собранные данные могли быть расшифрованы, проанализированы и использованы для постоянного дистанционного наблюдения этой группировки.

### Пример применения 2: Команда технического наблюдения

Команда технического наблюдения (КТН) следила за объектом, который часто посещал разные Интернет-кафе, из-за чего мониторинг с применением технологии типа троянского коня был невозможен. Средство FinUSB использовалось для извлечения **данных из использованных объектом терминалов общего пользования после его ухода**.

Можно было восстановить несколько документов, которые объект открыл в сайте своей веб-почты. В собранную информацию входили ключевые документы Office, журнал обозревателя, полученный путем анализа маркеров (cookies), и многое другое.

### Обзор функций

- Оптимизированная система для **скрытых операций**
- Легкая эксплуатация путем **автоматизированного выполнения**
- **Безопасное шифрование** с RSA и AES
- Извлечение **имен и паролей пользователей** по всем распространенным видам программного обеспечения, таким, как:
  - Клиенты электронной почты
  - Средства диалогового обмена сообщениями
  - Программы ускоренного просмотра
  - Средства дистанционного администрирования
- **Немое копирование файлов** (поиск дисков, корзины, последнего открытого/редактированного/созданного файла)
- Извлечение **сетевой информации** (записи обмена сообщениями, журнал обозревателя, ключи WEP/WPA(2), ...)
- Составление **системной информации** (применяемое/установленное программное обеспечение, информация о жестком диске, ...)

Пожалуйста, смотрите полный перечень функций в спецификации продукции.



**FINFISHER™**  
IT INTRUSION

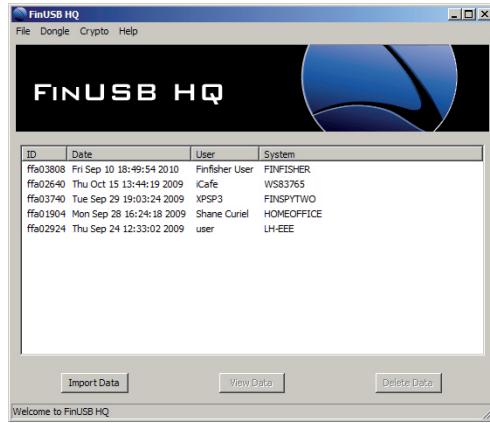
# Тактические средства IT проникновения

## НАБОР FINUSB SUITE

### СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



Набор «FinUSB Suite» – Переносная система



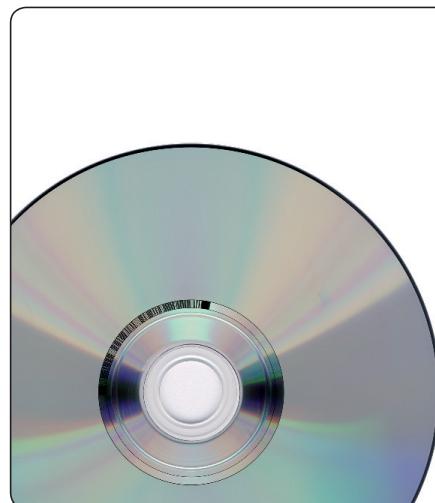
Виртуальный штаб «FinUSB HQ»

- Графический интерфейс пользователя для расшифровки и анализа собранных данных
- Конфигурация вариантов операционных действий аппаратного ключа



### 10 аппаратных ключей «FinUSB» (U3 - 16GB)

- Скрытое извлечение данных из системы
- Зашифровка данных на ходу



### FinUSB –Windows Password Bypass

- Обход регистрации Windows без постоянных системных модификаций

# Тактические средства IT проникновения

## НАБОР FINUSB SUITE

### ПРОСТАЯ ЭКСПЛУАТАЦИЯ



1. Взять аппаратный ключ FinUSB
2. Конфигурировать все нужные функции/модули и актуализировать Ваш аппаратный ключ FinUSB посредством виртуального штаба FinUSB HQ
3. Подойти к системе объекта
4. Вставить аппаратный ключ FinUSB
5. Подождать пока передаются данные
6. Возвратиться к штабу FinUSB HQ
7. Загрузить все данные с аппаратного ключа FinUSB
8. Составить отчет



### ПРОФЕССИОНАЛЬНЫЕ ОТЧЕТЫ

FINUSB HQ

FinUSB Suite: Report

I. Generic

Generic Information

II. Passwords

Windows Account Hashes  
E-Mail Accounts  
Messenger Accounts  
Google Chrome Passwords  
Firefox Passwords  
Network Passwords  
Protected Storage  
Internet Explorer Accounts

III. System

Windows Product Keys  
Windows Updates  
LSA Secrets  
Current Processes

IV. Network

Network Adapters  
Network Ports  
Internet Explorer History  
Mozilla Firefox History  
Wireless Keys  
Mozilla Firefox Cookies

Generic Information

Computer | Protected Mode: Off

75%



# Тактические средства IT проникновения

FINFIREWIRE

Отделения технического наблюдения и судебные эксперты часто встречаются с ситуацией, в которой им нужно иметь доступ к работающей компьютерной системе, не выключая ее, чтобы не потерять данные или критическое время при операции. В большинстве случаев система объекта защищена **скринсейвером с паролем**, или объект-пользователь еще не зарегистрировался и **экран входа в систему** еще действует.

Средство «FinFireWire» позволяет **оператору** быстро и скрыто **обойти защищенный паролем экран** и иметь доступ к системе объекта, при этом не оставляя следов и не повреждая необходимые судебные улики.

## Пример применения 1: Судебная операция

Команда судебных экспертов вошла в квартиру объекта и попыталась получить доступ к компьютерной системе. Компьютер был **включен, но экран был блокирован**. Данная команда не имела юридического права использовать средство дистанционного доступа, поэтому они **потеряли бы все данные**, если бы они выключили систему, поскольку **жесткий диск был полностью зашифрован**. Команда применила FinFireWire, чтобы **снять блокировку работающей системы объекта**, тем самым позволяя оператору **скопировать все файлы** перед тем, как выключить компьютер и забрать его в штаб.

## Обзор функций

- Разблокирует экран входа пользователя в систему для учетной записи всех пользователей
- Разблокирует скринсейвер с паролем
- Сбрасывает всю оперативную память RAM для криминалистического анализа
- Позволяет извлекать текущие судебные данные **без необходимости перезагружаться** в систему объекта
- Пароль пользователя **не изменяется**
- Поддерживает системы, работающие с Windows, Mac и Linux
- Работает с FireWire/1394, PCMCIA и Express Card
- Полный доступ ко **всем общим сетевым каталогам** пользователя

Пожалуйста, смотрите полный перечень функций в спецификации продукции.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	• Тактические операции
Возможности:	• Обход пароля пользователя • Скрытый доступ к системе • Восстановление пароля из оперативной памяти RAM • Позволяет извлечение текущих судебных данных
Содержание:	• Аппаратное оборудование и программное обеспечение

## Пример применения 2: Восстановление пароля

Объединив этот продукт с традиционными криминалистическими приложениями, такими как Encase®, команда судебных экспертов использовала функцию сброса оперативной памяти RAM, чтобы получить моментальный снимок текущей информации оперативной памяти RAM и на основании чего восстановила парольную фразу шифрования информации жесткого диска для шифрования всего диска TrueCrypt.



**FINFISHER™**  
IT INTRUSION

# Тактические средства IT проникновения

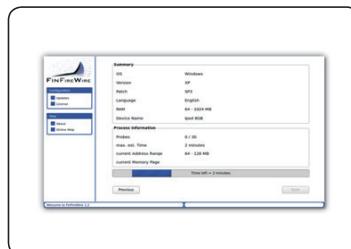
**FINFIREWIRE**

## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



### FinFireWire – Тактическое средство

- Укомплектованная тактическая система



### Интерфейс с использованием

- Простой в использовании пользовательский интерфейс



### Соединительные адаптерные платы

- Плата PCMCIA и ExpressCard для целевых систем без порта FireWire



### Набор универсальных кабелей FinWire

- 4-х контактный на 4-х контактный
- 4-х контактный на 6-ти контактный
- 6-ти контактный на 6-ти контактный

## ЭКСПЛУАТАЦИЯ



Содержанная в данном документе информация является конфиденциальной и может быть изменена без уведомления. Gamma Group International не несет ответственности за содержащиеся в этом документе технические или редакционные ошибки и опущения.



GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

[info@gammagroup.com](mailto:info@gammagroup.com)

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINSPY**

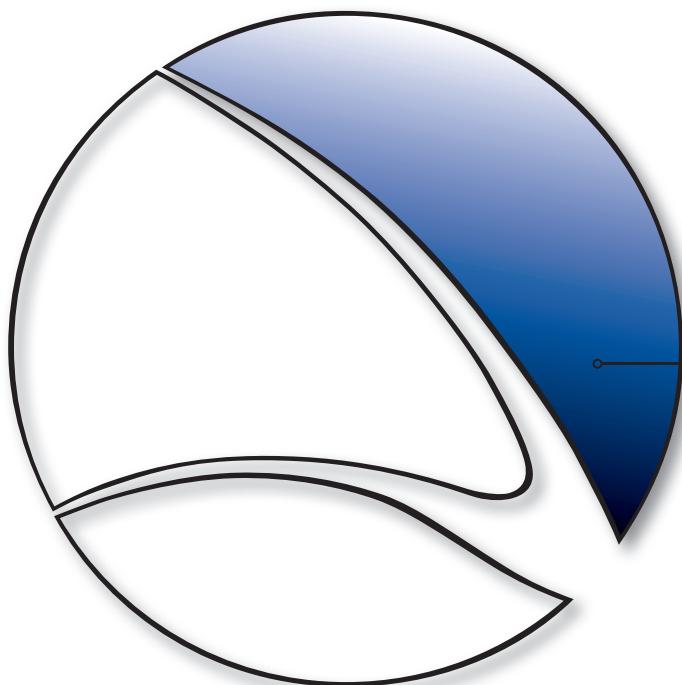
**FINSPY MOBILE**

**FINFLY USB**

**FINFLY LAN**

**FINFLY WEB**

**FINFLY ISP**



Средства дистанционного мониторинга и заражения применяются для того, чтобы получить доступ к системам и полный доступ к хранимой информации, и имеют возможность управлять функциями системы объекта до такой степени, что становится возможным извлечение зашифрованных данных и сообщений. При совместном применении с технологиями заражения, правительственные органы смогут дистанционно заражать целевые системы.



**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINSPY

«FinSpy» является проверенным на практике средством, позволяющим правительствам решать задачи осуществления **мониторинга мобильных объектов, осознающих важность сохранения своей безопасности**, которые часто **изменяют своё местонахождение, используют зашифрованные и анонимные средства связи**, и/или проживающие в **других странах**.

Традиционные средства законного перехвата связи **встречаются с новыми трудностями**, которые могут быть **решены только путем применения таких активных систем**, как «FinSpy»

- Данные не передаются по сетям
- Зашифрованная коммуникация
- Объекты в других странах

Система «FinSpy» **успешно применялась** в операциях по всему миру **на протяжении многих лет**, и была приобретена ценная разведывательная информация о намеченных личностях и организациях. При установке системы «FinSpy» в компьютере или сотовом телефоне появляется возможность **дистанционно контролировать и иметь к ним доступ**, как только они подключаются к Интернету/сети, **несмотря на то, в какой точке земного шара** находится система объекта.

## Обзор функций

Объектный компьютер – примеры функций:

- Обход 40 регулярно проверяемых антивирусных систем
- **Скрытая связь** со штабом
- Полный мониторинг по «Skype» (звонки, обмен сообщениями, передача файлов, видеосвязь, список контактов)
- Запись **распространяемых средств связи**, таких, как электронная почта, обмен сообщениями и VoIP
- **Мониторинг в реальном масштабе времени** через веб-камеру и микрофон
- **Прослеживание объекта по странам**
- **Немое извлечение файлов** с жесткого диска
- Более быстрый анализ благодаря **программе, основанной на процессах, для перехвата вводимой с клавиатуры информации**
- Удаленная криминалистическая **экспертиза системы объекта в реальном времени**
- **Современные фильтры** для записи только важной информации
- Поддержка стандартных операционных систем (**Windows, Mac OSX и Linux**)

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	Тактические операции
Возможности:	<ul style="list-style-type: none"><li>Сбор информации Доступ к системам</li><li>Быстрое извлечение судебной информации</li></ul>
Содержание:	Аппаратное оборудование и программное обеспечение

## Пример применения 1: Разведывательное управление

Система «FinSpy» была установлена в нескольких компьютерных системах, находящихся в **Интернет-кафе в критических местах** для того, чтобы наблюдать за совершаемыми на них подозрительными действиями, особенно за **связью по системе «Skype»** с иностранными лицами. С помощью использования веб-камеры сделали фотографии объектов в то время, как они работали с данными системами.

## Пример применения 2: Организованная преступность

Система FinSpy была **скрытно запущена на системах объекта** нескольких членов группы организованной преступности. На основании **использования инструментов отслеживания объекта по странам и доступа к удаленному микрофону**, можно собрать важную информацию от **каждого совещания, проведенного этой группой**.

Виртуальный штаб – примеры функций:

- Сохранение улик (допустимые по **Европейским стандартам улики**)
- Управление пользователями согласно проверке безопасности
- Безопасность зашифрованных данных и связи по **RSA 2048 и AES 256**
- Скрытие от посторонних через **анонимные прокси**
- **Может быть полностью интегрируемым** с правоохранительными системами.

Пожалуйста, смотрите полный перечень функций в спецификации продукции.



**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINSPY**

## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



### FinSpy Master и Proxy

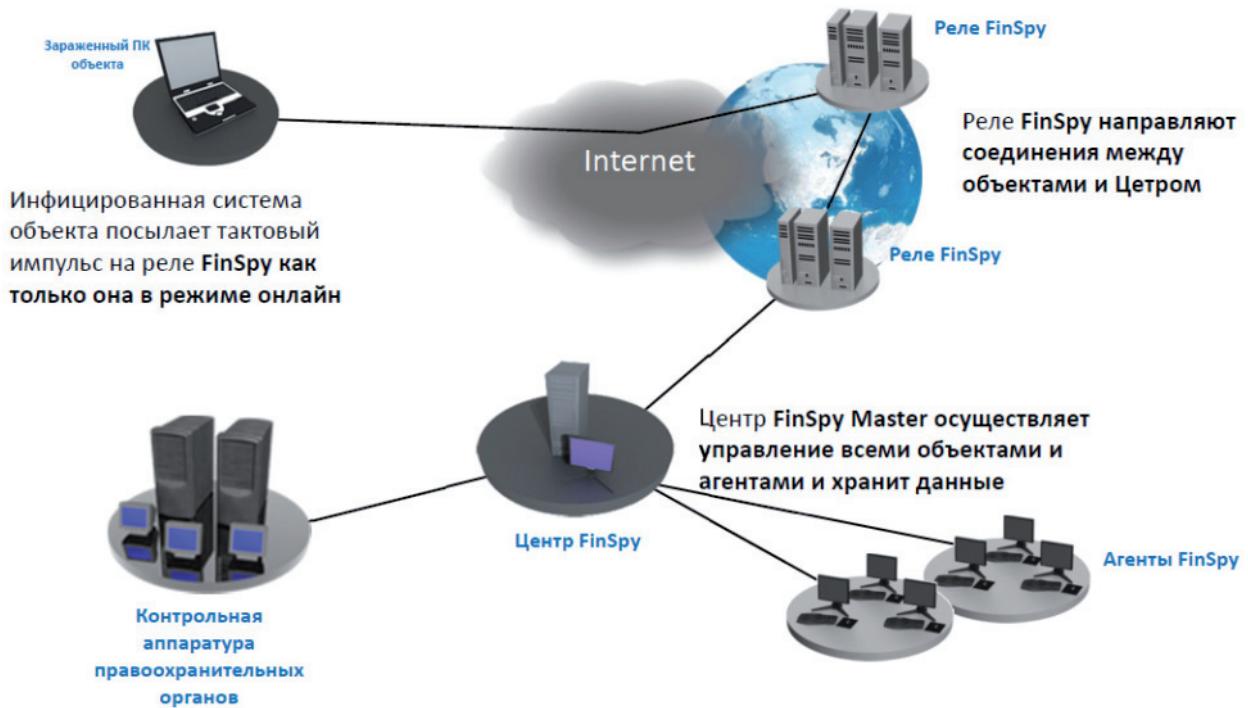
- Полный контроль систем объекта
- Сохранение улик по данным и журналам операций
- Надежное сохранение информации
- Управление пользователями и объектами, основанное на проверке безопасности



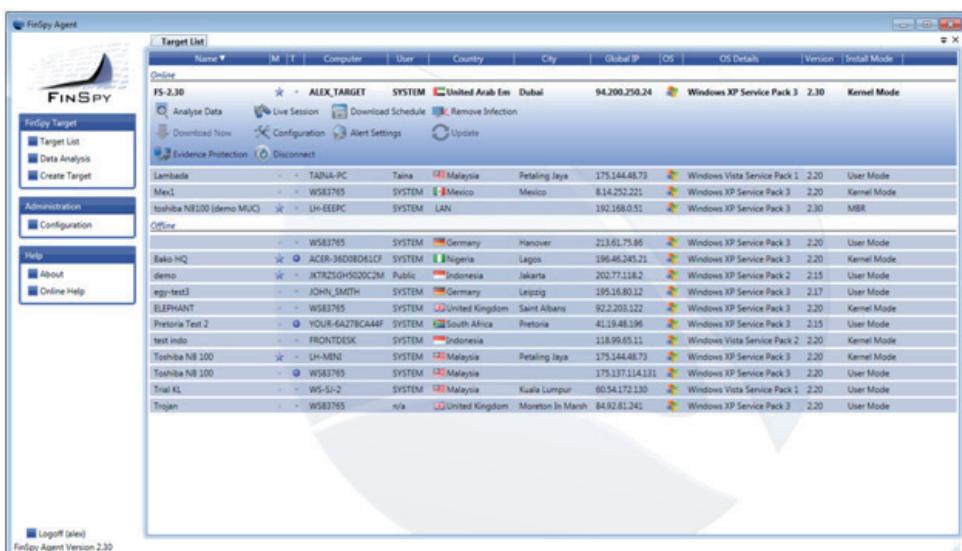
# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINSPY**

## ДОСТУП К КОМПЬЮТЕРНЫМ СИСТЕМАМ ОБЪЕКТА ПО ВСЕМУ МИРУ



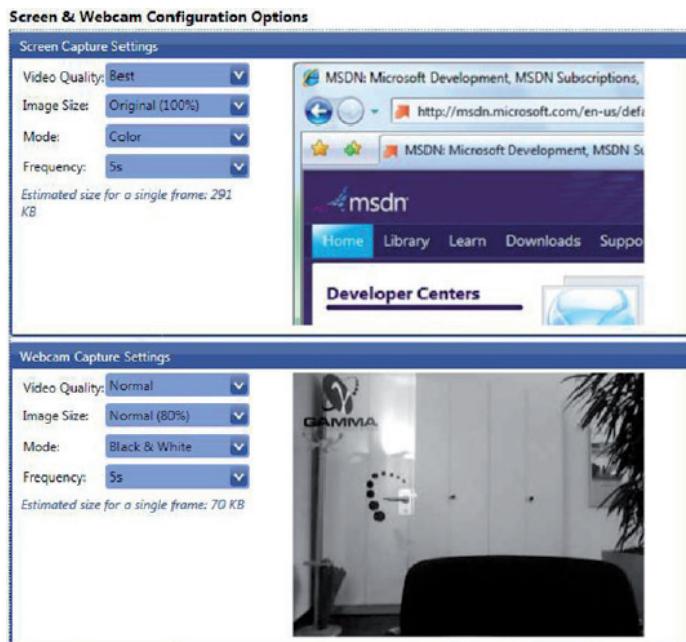
## ПРОСТОЙ В ИСПОЛЬЗОВАНИИ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINSPY

## КОНФИГУРАЦИИ ОБЪЕКТОВ В РЕАЛЬНОМ МАСШТАБЕ ВРЕМЕНИ И В РЕЖИМЕ ОФЛАЙН



## ПОЛНАЯ РАЗВЕДЫВАТЕЛЬНАЯ ИНФОРМАЦИЯ ПО СИСТЕМЕ ОБЪЕКТА



1. Широкий обзор многокомпонентных данных
2. Анализ структурированных данных
3. Уровни важности для всех записанных файлов

Содержанная в данном документе информация является конфиденциальной и может быть изменена без уведомления. Gamma Group International не несет ответственности за содержащиеся в этом документе технические или редакционные ошибки и опущения.



GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

info@gammagroup.com

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

## ЛИЦЕНЗИИ FINSPY

### ОБЩАЯ ИНФОРМАЦИЯ

Средства FinSpy включают 3 типа лицензий:

#### A. Лицензия на корректировку

Лицензия на корректировку контролирует способность **FinSpy** осуществлять выборку новых откорректированных данных из сервера обновления Gamma. Она объединена с модулем **послепродажной поддержки FinFisher™**.

По истечению срока действия, система **FinSpy** будет оставаться **полностью функциональной**, но не сможет больше осуществлять выборку новейших версий и устранения ошибок с сервера обновления FinSpy.

#### B. Лицензия агента

Лицензия агента контролирует количество агентов **FinSpy**, которые могут входить в **главную систему FinSpy Master** параллельно.

Пример:

- закуплено **5 лицензий агента**.
- **Лицензии агента FinSpy** могут быть установлены на неограниченном количестве систем, однако
- Только **5 систем FinSpy агента** могут входить в **систему FinSpy Master и работать с данными в системе** одновременно.

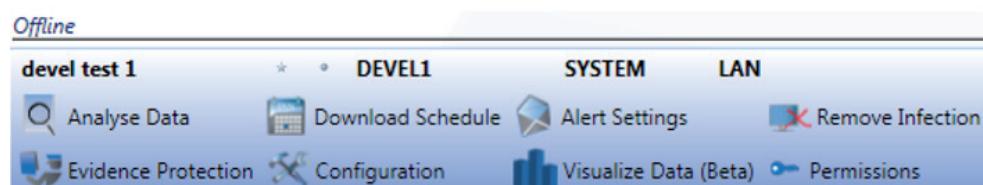
#### C. Лицензия объекта

Лицензия объекта контролирует количество объектов **FinSpy**, которые могут быть задействованными одновременно.

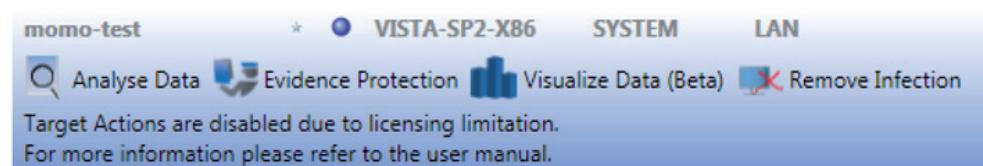
"**Задействованный**" означает **активированные инсталляции объекта FinSpy**, независимо от того находятся ли они в режиме онлайн или офлайн.

В случае, если объект **FinSpy** развернут на систему объекта без наличия лицензий объекта, **объект FinSpy** временно деактивируется, что исключает возможность записи или доступа. Сразу же, после появления новой лицензии (например, продления срока существующей лицензии или обеззараживания одного из активных объектов **FinSpy**), объекту будет присвоена свободная лицензия и он будет активирован, чтобы начать запись и обеспечить доступ в реальном времени.

### СНИМОК ЭКРАНА АКТИВИРОВАННОЙ ЦЕЛИ С ЛИЦЕНЗИЕЙ



### СНИМОК ЭКРАНА ДЕЗАКТИВИРОВАННОЙ ЦЕЛИ БЕЗ ЛИЦЕНЗИИ



**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

## СИСТЕМА FINSPY MOBILE

FinSpy Mobile заполняет пробел в возможностях перехвата информации для правительственные организаций для большинства **платформ интеллектуальных телефонов**.

В частности, организации, не имеющие возможности **перехвата сети или систем без выхода в эфир**, могут получить доступ к мобильным телефонам и перехватывать устройства на основании усовершенствованных возможностей. Более того, предлагается **решение доступа к шифрованной связи** и также к непередаваемым данным, **сохраненным на устройствах**.

Традиционные тактические или стратегические решения перехвата **встречаются с проблемами**, которые могут быть решены только на основании **использования агрессивных систем**, таких как FinSpy Mobile:

- Данные, не передаваемые ни по каким сетям и хранящиеся на устройстве
- Шифрованная связь в радио-интерфейсе, при которой избегается использование тактических активных или пассивных систем без выхода в эфир
- Межабонентское шифрование с таких устройств как программы обмена сообщениями Messenger, электронная почта или PIN сообщения.

Система FinSpy Mobile доказала свою успешность при использовании правительственными организациями, которые собирают информацию дистанционно с мобильных телефонов объекта.

### Обзор функций

Виртуальный штаб – примеры функций:

- **Засекреченная связь** со штабом
- Запись **стандартных видов связи**, таких как голосовой вызов, SMS/MMS и э-почта
- **Наблюдение в реальном времени** посредством немых звонков
- **Загрузка файлов** (перечней контактов, календарь, фотографии, файлы)
- **Определение страны местонахождения объекта** (посредством GPS и идентификационного номера сотового телефона)
- Полная запись **всей связи через BlackBerry Messenger**
- Поддержка большинства стандартных операционных систем: **Windows Mobile, iOS (iPhone), BlackBerry и Android**

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	<ul style="list-style-type: none"><li>• Стратегические операции</li><li>• Тактические операции</li></ul>
Возможности:	<ul style="list-style-type: none"><li>• Дистанционный мониторинг сотового телефона</li></ul>
Содержание:	<ul style="list-style-type: none"><li>• Аппаратное оборудование и программное обеспечение</li></ul>

При установке FinSpy Mobile на мобильном телефоне, его можно контролировать и проверять дистанционно, независимо от местонахождения объекта где-либо в мире.

### Пример применения 1: Разведывательная организация

FinSpy Mobile была установлена на мобильных телефонах **BlackBerry** нескольких объектов для контроля связи, включая **SMS/MMS, э-почту и программы обмена сообщениями BlackBerry Messenger**.

### Пример применения 2: Организованная преступность

FinSpy Mobile была скрытно установлена на мобильных телефонах нескольких членов группы организованной преступности (ГОП). На основании использования данных **слежения GPS и немых звонков**, можно было собрать важную информацию **с каждой встречи, организованной этой группой**.

Штаб – примеры функций:

- Защита фактических данных (законные фактические данные в соответствии с **Европейскими стандартами**)
- Управление абонентской системой в соответствии с допуском к секретной информации
- Шифрование секретной информации и связь с использованием **RSA 2048 и AES 256**
- Скрытие от общественности посредством **анонимности прокси-сервера**
- Способность **полной интеграции** с функциями контроля правоохранительных органов

Пожалуйста, смотрите полный перечень функций в спецификации продукции



**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

## FINSPY MOBILE

### СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



#### FinSpy Master и Proxy

- Полный контроль телефонов объекта
- Защита фактической информации для регистрационных журналов данных и операций
- Надежное хранение
- Проверка на отсутствие нарушения секретности на основании управления пользователем и объектом

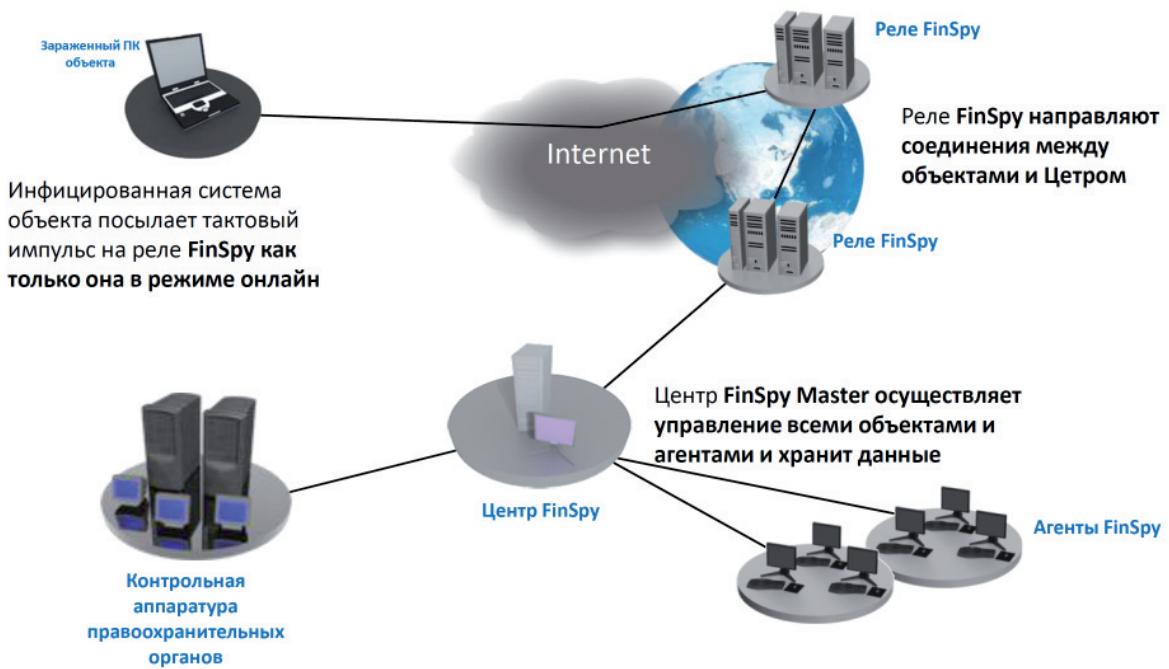
#### FinSpy Agent

- Графический интерфейс пользователя для сеансов в реальном времени, конфигурация и анализ данных объектов

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

## FINSPY MOBILE

### ДОСТУП К МОБИЛЬНЫМ ТЕЛЕФОНАМ ОБЪЕКТА ПО ВСЕМУ МИРУ



### УДОБСТВО РАБОТЫ С ПОЛЬЗОВАТЕЛЬСКИМ ИНТЕРФЕЙСОМ

The screenshot displays the FINSPY MOBILE user interface. The top navigation bar includes links for Target Account, Configure, Event Report, Remote Command, License, Custom Report, and Logout (admin). The main area is titled "Event Report" and shows a table of results. The table has columns for Select, Flag, Entry, Type, Direction, Contact, Duration, Details, Mobile Time, and Server Time. The "ALL (20)" button is highlighted. The table lists 20 entries, each with a checkbox, a flag value, an entry ID, a type (IM), a direction (Outgoing or Incoming), a contact email, a duration, and two timestamp columns.

Select	Flag	Entry	Type	Direction	Contact	Duration	Details	Mobile Time	Server Time
	40	Im	Outgoing	User <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	39	Im	Outgoing	User <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	38	Im	Incoming	Phoenix <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	37	Im	Outgoing	User <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	36	Im	Incoming	Phoenix <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	35	Im	Incoming	Phoenix <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05
	34	Im	Incoming	Phoenix <phoenix@email.com>				2010-October-06 02:28:05	2010-October-13 06:11:05



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINFLY USB**

Универсальная последовательная проводная шина FinFly USB обеспечивает удобный и надежный способ установки средств дистанционного контроля на компьютерных системах при наличии физического доступа к ним.

После введения FinFly USB в компьютер, **она автоматически устанавливает конфигурированную программу** с незначительным участием или совсем без участия пользователя, **не требуя специального обучения операторов-агентов**. FinFly USB может быть использована против **множества систем** до возвращения ее в штаб.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	· Тактические операции
Возможности:	· Разворачивает дистанционные средства контроля на объекте
Содержание:	· Аппаратное оборудование

## Пример применения 1: Группа технического наблюдения

FinFly USB нашла успешное применение **в группах технического наблюдения** в нескольких странах для внедрения средств дистанционного контроля в системы объекта, которые были **выключены**, посредством простой загрузки **системы с устройства FinFly USB**.

## Пример применения 2: Разведывательное управление

Источнику информации в национальной террористической группировке было вручено FinFly USB, который **скрытно установил средство дистанционного мониторинга** на нескольких компьютерных системах данной группировки при его использовании членами группы для передачи документов между собой. После проведения такой операции, появилась **возможность дистанционного контроля систем объекта со штаба**, после чего источник вернул устройство FinFly USB.

## Обзор функций

- Скрыто устанавливает средство дистанционного мониторинга при вводе в систему объекта
- Требует **незначительного участия** или совсем **никакого участия** со стороны пользователя
- Можно скрывать функциональность устройства записью на нём обычных файлов, таких, как музыка, видеозаписи и документы
- Заражение выключеной системы объекта при загрузке с USB
- Аппаратное оборудование является **обычным, не вызывающим подозрение, устройством USB**

Пожалуйста, смотрите полный перечень функций в спецификации продукции



**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINFLY USB**

## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



### **FinFly USB**

- Аппаратный ключ SanDisk USB
- Устанавливает средство дистанционного мониторинга при вводе в системы объекта
- Устанавливает средство дистанционного мониторинга во время процесса загрузки

### **Полная интеграция FinSpy**

- Автоматическое создание и активизация посредством FinSpy Agent

Содержанная в данном документе информация является конфиденциальной и может быть изменена без уведомления. Gamma Group International не несет ответственности за содержащиеся в этом документе технические или редакционные ошибки и опущения.



GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

[info@gammagroup.com](mailto:info@gammagroup.com)

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY LAN

Одной из главных задач правоохранительных органов являются **мобильные объекты**, где **физический доступ** к компьютерной системе **невозможен** и посланные по электронной почте **зараженные файлы** не открываются объектами.

В частности, **фактически невозможно** заражать объекты, осознающие важность сохранения своей безопасности из-за того, что они **постоянно возобновляют защиту** своих систем, вследствие чего **невозможно находить слабые** места, в связи с чем стандартные технологии проникновения оказываются безуспешными.

Система FinFLy LAN была разработана для скрытого развертывания средств дистанционного мониторинга в системах объекта в локальной компьютерной сети (проводной и беспроводной/802.11). Данная система может **заражать файлы**, загружаемые объектом на ходу, **отправлением фальшивых обновлений** популярного программного обеспечения или заражать объект посредством **ввода полезных данных в посещаемые сайты**.

## Пример применения 1: Группа технического наблюдения

Группа технического наблюдения следила за объектом на протяжении нескольких недель без возможности получить физический доступ к его компьютеру. Члены группы использовали систему FinFLy LAN для установки средства дистанционного мониторинга в системе объекта, когда он использовал **общественную точку доступа** в кафе.

## Обзор функций

- **Обнаруживает все** подключенные к локальной сети **компьютерные системы**
- Работает в **проводных и беспроводных (802.11)** сетях
- Может быть совмещен с набором FinIntrusion Kit **для скрытого доступа к сетям**
- Скрывает средство дистанционного мониторинга в **загруженных файлах объекта**
- Вводит средство дистанционного мониторинга, такое, как **обновление программного обеспечения**
- Дистанционная установка средства дистанционного мониторинга через посещаемые объектом веб-

Пожалуйста, смотрите полный перечень функций в спецификации продукции

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	· Тактические операции
Возможности:	· Разворачивает средство дистанционного мониторинга в системе объекта в локальной компьютерной сети
Содержание:	· Программное обеспечение

## Пример применения 2: Борьба с коррупцией

Система FinFLy LAN использовалась для установки средства дистанционного мониторинга в компьютер объекта, в то время как он использовал его в **своем гостиничном номере**. Операторы, находящиеся в другом номере, **подключились к той же сети** и манипулировали посещаемыми объектом веб-сайтами, чтобы запустить установку.

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINFLY LAN**

## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



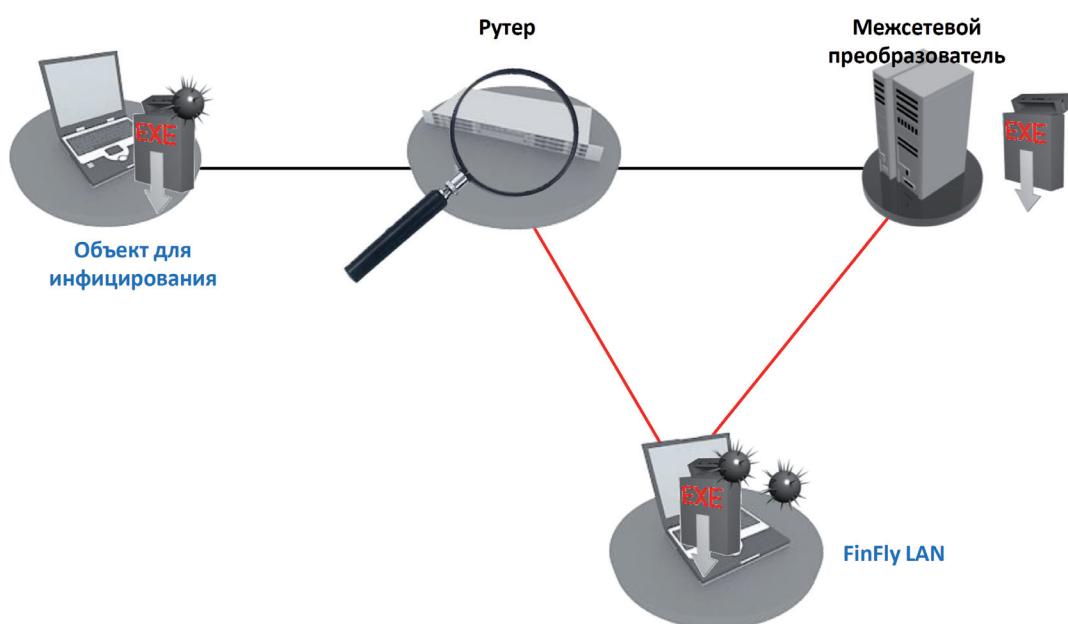
### FinFly LAN

- Основанное на «Linux» программное обеспечение с простым интерфейсом пользователя

### Комплект FinIntrusion Kit - интеграция (не входит в базовый комплект)

- FinFly LAN может быть установлен как модуль в комплекте FinIntrusion Kit

## ЗАРАЖЕНИЕ ЧЕРЕЗ ЛОКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ



### АВТОМАТИЗИРОВАННЫЙ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

- Простой в использовании без необходимости обширной подготовки

Systems Infected			
Target identifier	Payload	InfectionMethod	Infected at
testuser5	test_trojan_1.exe	Binary	20:30:12 27/08/2010
10.0.0.52	test_trojan_2.exe	Update	16:12:37 23/08/2010

### ПОДДЕРЖКА ДЛЯ МНОГОЧИСЛЕННЫХ ОБЪЕКТОВ И ПОЛЕЗНЫХ ДАННЫХ

- Разные исполняемые модули могут быть добавлены для каждого объекта

**Infection Techniques**

Binary Infection(.exe,.scr)

Operation mode:



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY WEB

Одной из главных задач при использовании средства дистанционного мониторинга является его внедрение в систему объекта, особенно когда имеется мало информации, такой, как **адрес электронной почты и нет физического доступа**.

Система FinFly Web разработана для **дистанционного и скрытого** заражения системы объекта помощью применения широкого диапазона **атак по Интернету**. Система FinFly Web предоставляет **интерфейс типа «укажи и выбери»**, позволяющий оператору легко **создать специализированный заражающий код** по выбранным модулям.

Системы объекта, посещающего подготовленные веб-сайты с внедренным заражающим кодом, будут **скрыто заражены** сконфигурированным программным обеспечением.

## Пример применения 1: Команда технического наблюдения

После профилирования объекта, команда создала **интересующий объекта веб-сайт** и послала ему ссылку через **форум**. При открытии ссылки на веб-сайт команды, средство дистанционного мониторинга было внедрено в систему объекта, и **мониторинг объекта можно было осуществлять из штаба**.

## Обзор функций

- Полностью приспособляемые веб-модули
- Скрытая установка в каждом веб-сайте
- Полная интеграция с «FinFly LAN» и «FinFly ISP» для установки даже в популярных веб-сайтах, таких, как веб-почта, видео-порталы и многих других
- Установка средства дистанционного мониторинга даже в случае, если известен только адрес электронной почты
- Возможность выбрать любого посетителя сконфигурированных веб-сайтов

Пожалуйста, смотрите полный перечень функций в спецификации продукции

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	· Стратегические операции
Возможности:	· Устанавливает средство дистанционного мониторинга в системе объекта через веб-сайты
Содержание:	· Программное обеспечение

## Пример применения 2: Развведывательная организация

Клиент установил систему **FinFly ISP** у **главного провайдера услуг Интернета** своей страны. Данная система была **скомбинирована с FinFly Web** для **дистанционного заражения объектов, посещающих оскорбляющие правительство веб-сайты**, путем ввода кода FinFly Web в веб-сайты объекта.

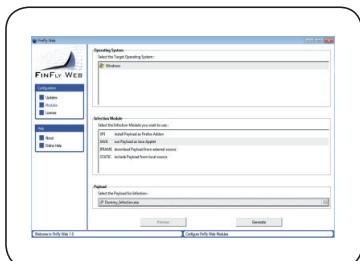


**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINFLY WEB**

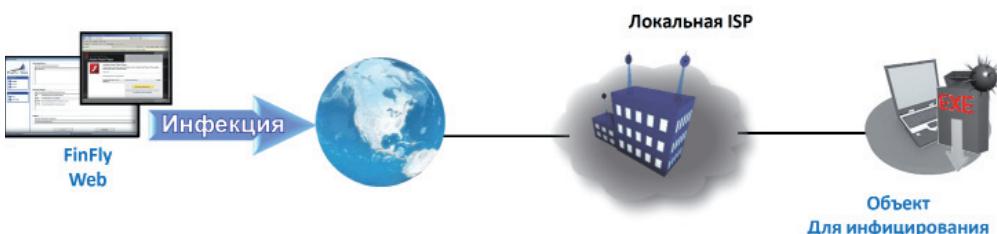
## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ



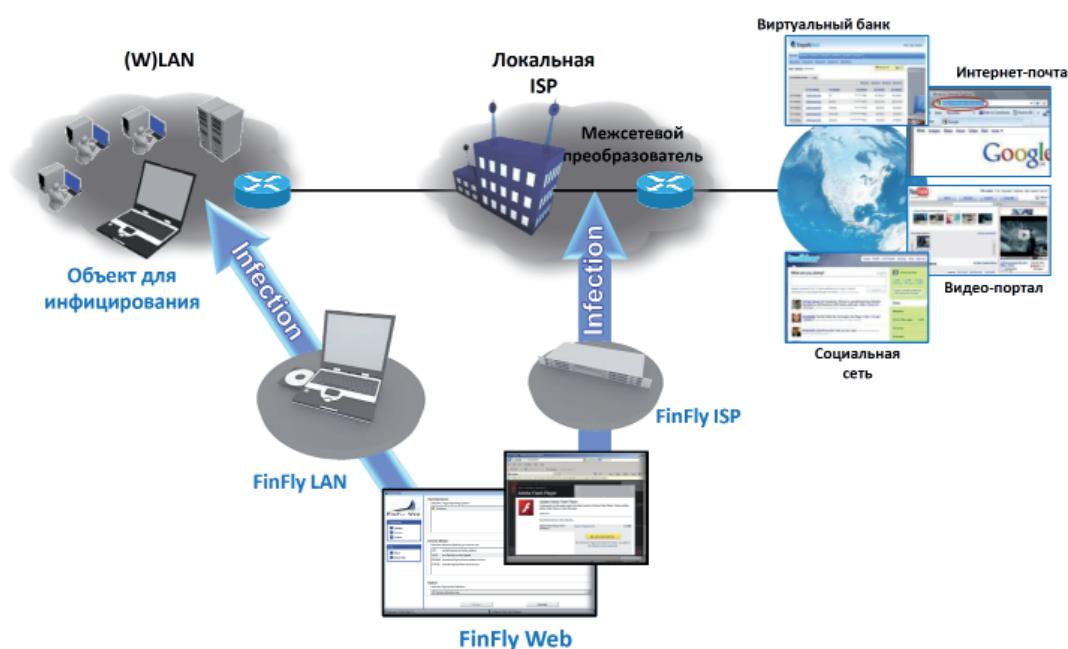
### FinFly Web

Программное обеспечение типа «укажи и выбери» для создания специализированных заражающих веб-сайтов

## НЕПОСРЕДСТВЕННОЕ ЗАРАЖЕНИЕ СИСТЕМОЙ «FinFly WEB»



## ПОЛНАЯ ИНТЕГРАЦИЯ С «FinFly LAN» И «FinFly ISP»



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY WEB

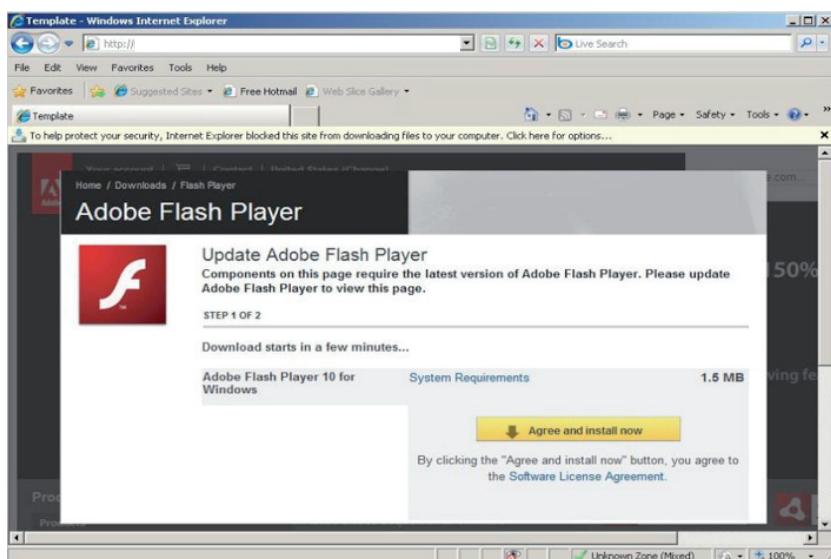
## Пример: Example: Java-приложение (Internet Explorer, Firefox, Opera, Safari)

Веб-сайт запросит объект принять Java-подключаемый модуль, который может быть подписан названием любой компании (напр. «Microsoft Corporation»)



## Пример: Отсутствующий компонент (IE, Firefox, Opera, Safari)

Веб-сайт симулирует, что определенный подключаемый модуль/кодер-декодер отсутствует в системе объекта и запросит систему загрузить и установить недостающее программное обеспечение.

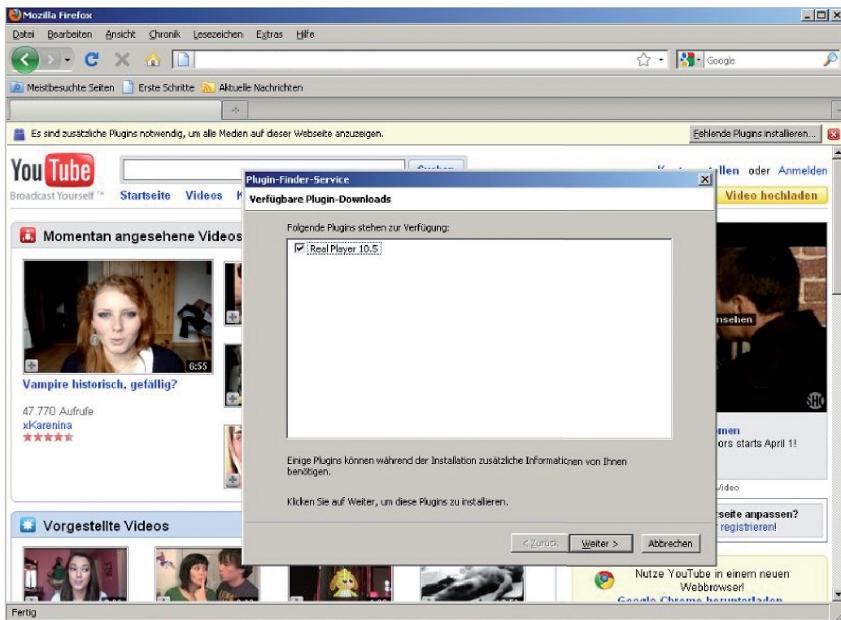


# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY WEB

## Пример: Отсутствующий межплатформенный инсталлятор (только Firefox, все платформы)

Данный модуль запросит объект установить дополнительные подключаемые модули, чтобы обеспечить возможность просмотра веб-сайта.



Содержанная в данном документе информация является конфиденциальной и может быть изменена без уведомления. Gamma Group International не несет ответственности за содержащиеся в этом документе технические или редакционные ошибки и опущения.



GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

info@gammagroup.com

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY ISP

Во многих реальных операциях, физический доступ к системам объекта внутри страны невозможен и требуется скрытая **дистанционная установка** средства дистанционного мониторинга для того, чтобы осуществлять мониторинг объекта из штаба.

Система FinFly ISP является стратегическим, **овхватившим всю страну, и тактическим** (мобильным) средством, **интегрируемым в сети доступа и/или опорной сети провайдера услуг Интернета** для дистанционной установки средства дистанционного мониторинга в выбранных системах объекта.

Устройства FinFly ISP основываются на **серверной технологии операторского класса** и обеспечивают максимальную **надежность и расширяемость** для решения каждой, связанной с сетевыми топологиями задачей. Широкий диапазон сетевых интерфейсов, **защищаемых обходными функциями**, предоставляется для требуемой подключаемости к активным сетям.

Некоторые пассивные и активные технологии для идентификации объекта – от **мониторинга в режиме «онлайн»** путем пассивного **подключения к интерактивной связи** между FinFly ISP и AAA-серверами – обеспечивают идентификацию объектов и предоставление соответствующего трафика для процесса заражения.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	• Стратегические операции
Возможности:	• Устанавливает средство дистанционного мониторинга в системе объекта через сеть провайдера услуг Интернета
Содержание:	• Аппаратное оборудование и программное обеспечение

Система FinFly ISP может **зарождать** загружаемые объектом **файлы** на ходу или заражать систему объекта путем **отправки фальшивых обновлений** популярного программного обеспечения. Новая версия теперь интегрирует мощную дистанционную программу Gamma в FinFly Web для заражения объектов на ходу при посещении любых веб-сайтов.

## Пример применения: Разведывательная организация

Система FinFly ISP была установлена в сетях главного провайдера услуг Интернета страны и активно применялась для дистанционной установки средства дистанционного мониторинга в системах объекта. Идентификация объектов была установлена по их регистрационным именам Radius благодаря тому, что объекты имели DSL счет с динамическим IP.

## Обзор функций

- Устанавливается в сети провайдера услуг Интернета
- Работает со **всеми распространенными протоколами**
- Объекты выбираются по **IP адресу или регистрационному имени Radius**
- Средство дистанционного мониторинга **скрыто в перекачках объекта**
- Введение средства дистанционного мониторинга в виде **обновления программного обеспечения**
- Дистанционная установка средства дистанционного мониторинга через посещаемые объектом веб-сайты

Пожалуйста, смотрите полный перечень функций в спецификации продукции



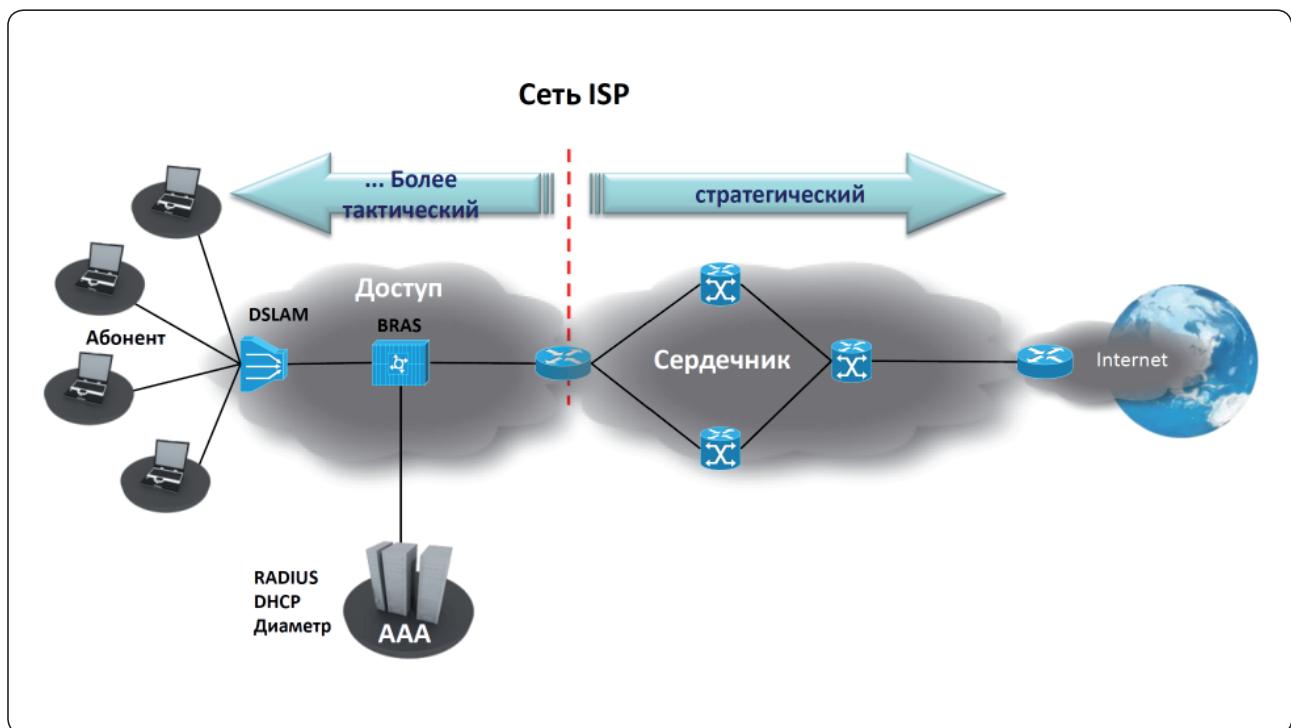
**FINFISHER™**  
IT INTRUSION

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FINFLY ISP

## ВОЗМОЖНЫЕ МЕСТА УСТАНОВКИ

- Система FinFly ISP может быть использована в качестве тактического и стратегического средства в сетях провайдера услуг Интернета



Тактическое средство является мобильной системой и его аппаратное оборудование предназначено для задач заражения в сети доступа близко к точкам доступа объекта. Оно может быть установлено на короткий период, чтобы решить тактические задачи, сфокусированные на конкретный объект или конкретное количество объектов в определенном месте.

Стратегическое средство является постоянной общегосударственной установкой FinFly ISP у провайдера услуг Интернета для подбора и заражения любого объекта с дистанционного штаба без необходимости нахождения правоохранительных органов непосредственно у объектов.

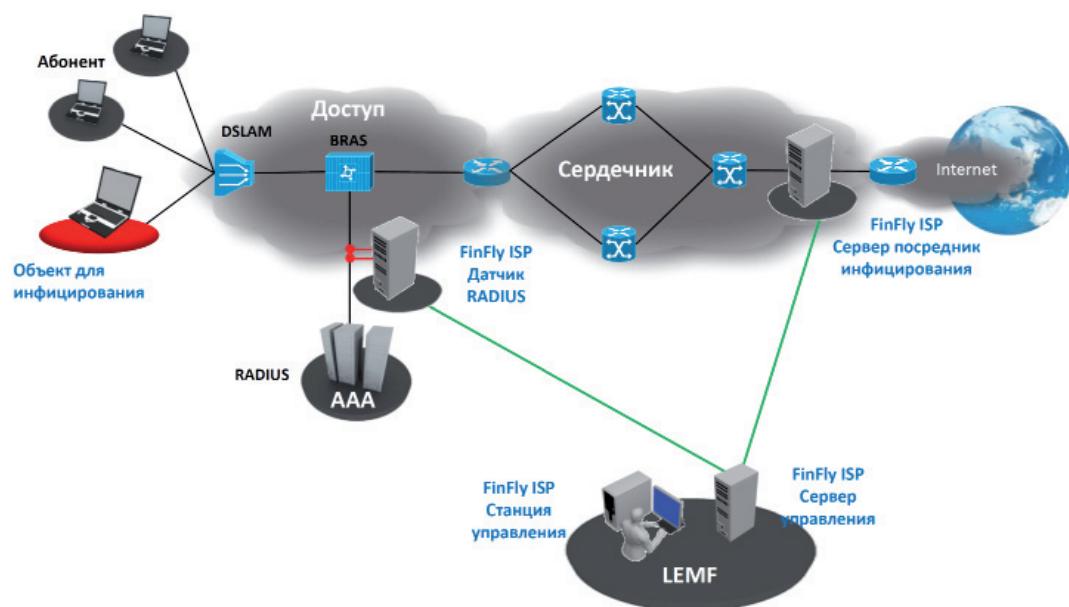
Конечно, возможно совместно использовать тактическое и стратегическое средства, чтобы оптимизировать приспособляемость систем при операциях заражения.

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

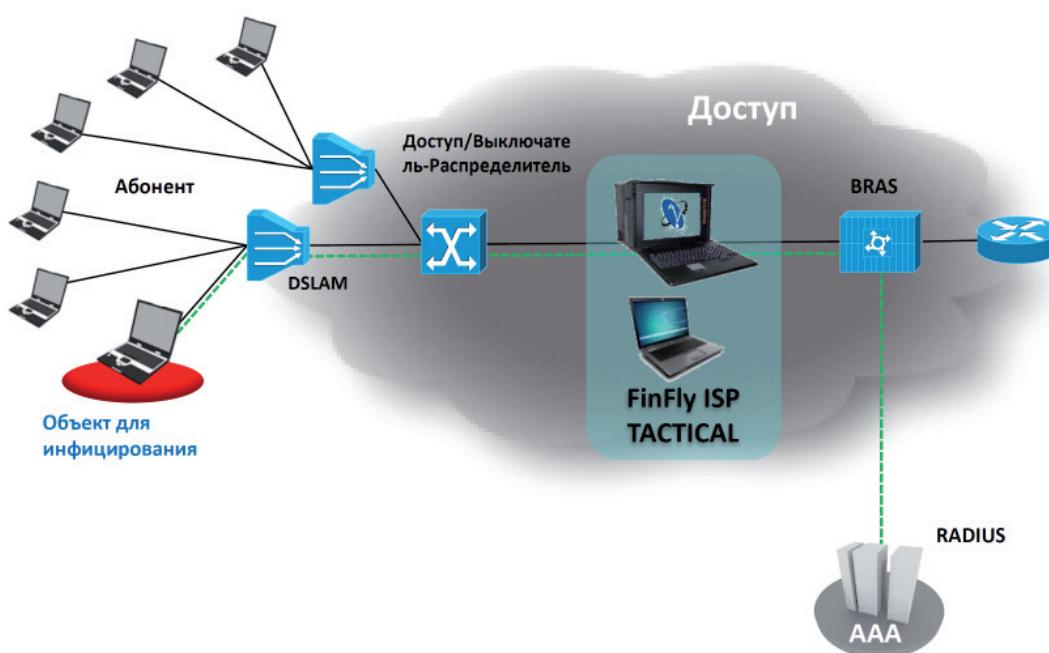
**FINFLY ISP**

## УСТАНОВКА СЕТИ

### Стратегическое развертывание



### Тактическое развертывание



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FINFLY ISP**

## СОСТАВНЫЕ ЧАСТИ ПРОДУКЦИИ

### Минимальный состав для стратегического развертывания FinFly ISP включает следующее:

- Система управления на LEMF (контрольной аппаратуре правоохранительных органов)
- Сервер (ы) датчика идентификации объекта системы AAA в сети
- Сервер(ы) – посредник(и) инфекции, например на межсетевом преобразователе(ах).

#### Серверы FinFly ISP

#### Рабочая Станция

HP ProLiant DL-Series G7  
Business WS



#### FinFly ISP

#### HP Z-Series

HP Z-Series



### Тактическая система FinFly ISP

Состоит из следующего:

- Идентификация цели и портативный сервер-посредник инфекции
- Портативный компьютер системы управления

#### FinFly ISP Tactical

#### переносное управление

Atlas A9 17" Portable



#### FinFly ISP Tactical

#### Lenovo Thinkpad

T-Series



Технические данные / спецификации могут быть изменены без уведомления

Пропускная способность	20 Gbps
Максимальное количество сетевых интерфейсных карт:	2-8
Интерфейсы:	1GE медь/ волокно 10GE медь / волокно SONET/SDH OC-3 / -192 STM-1 / -64 ATM AAL5
Процессоры:	1x – 8x Intel XEON
Магнитный сердечник:	2—8 сердечников / процессор
RAM:	12 GB – 1 TB
Емкость жесткого диска (HDD):	3x 146GB – 4.8TB SAS
Характеристика:	HP iLO 3 Избыточное питание Избыточная вентиляция Функция вспомогательного выключателя (если установлена)
Операционная система:	Linux GNU (Debian 5.0) защищенная

Пропускная способность	5 Gbps
Максимальное количество сетевых интерфейсных карт:	3
Интерфейсы:	1GE медь/ волокно SONET/SDH OC-3 / -12 STM-1 / -4 ATM AAL5
Процессоры:	2 x Intel – сердечника i7
Магнитный сердечник:	6 сердечников / процессор
RAM:	12 GB
Емкость HDD:	2 x 1TB SATA
Оптический привод:	DVD+/-RW SATA
Монитор:	1 x 17" TFT
Характеристика:	Функция вспомогательного выключателя для Центров сетевой информации (NIC)
Операционная система	Linux GNU (Debian 5.0) защищенная

Содержанная в данном документе информация является конфиденциальной и может быть изменена без уведомления. Gamma Group International не несет ответственности за содержащиеся в этом документе технические или редакционные ошибки и опущения.



GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

[info@gammagroup.com](mailto:info@gammagroup.com)

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА FINSUPPORT

### ТЕХНИЧЕСКАЯ ПОДДЕРЖКА FINSUPPORT

FinSupport поддерживает процессы модернизации и усовершенствования номенклатуру выпускаемых изделий FinFisher™ в сочетании с ежегодным контрактом на обслуживание.

Группа поддержки через веб-портал и группу технической поддержки FinFisher™ предоставляют следующие услуги своим клиентам:

- Онлайновый доступ к:
  - последним версиям руководства пользователя
  - последним версиям спецификаций продукции
  - последним версиям обучающих слайдов
  - внешнему интерфейсу отчета об ошибках
  - внешнему интерфейсу запроса свойств
- Регулярное обновление программного обеспечения:
  - Устранение ошибок
  - Новые свойства
  - Новые основные версии
- Техническая поддержка через Skype:
  - Устранение ошибок
  - Частичная операционная поддержка

#### Техническая поддержка FinLifelineSupport

FinLifelineSupport обеспечивает профессиональную поддержку, предоставляемую инженерным персоналом при решении проблем и технических вопросов. Кроме того, предоставляется профессиональная поддержка дистанционно при устранении ошибок программного обеспечения FinFisher™ и замене гарантийного аппаратного оборудования. В дополнение, при поддержке FinLifelineSupport клиент автоматически получает обновления новых свойств и функций вместе со стандартным релизом отладочных компонентов.

#### Устранение ошибок

FinSupport является организацией, предоставляющей поддержку по специальной продукции посредством высококвалифицированного персонала, отвечающего за послепродажную поддержку, когда менеджер получает вопросы по э-поште или телефону. Менеджер послепродажной поддержки базируется в Германии; его часы работы: 09:00 – 17:00 центрально-европейское время (ЦЕВ).

Рабочие часы FinLifelineSupport: 09:00–17:00 (ЦЕВ). В случаях поступления запроса о поддержке вне стандартных часов работы, запрос обрабатывается немедленно в следующий рабочий день.

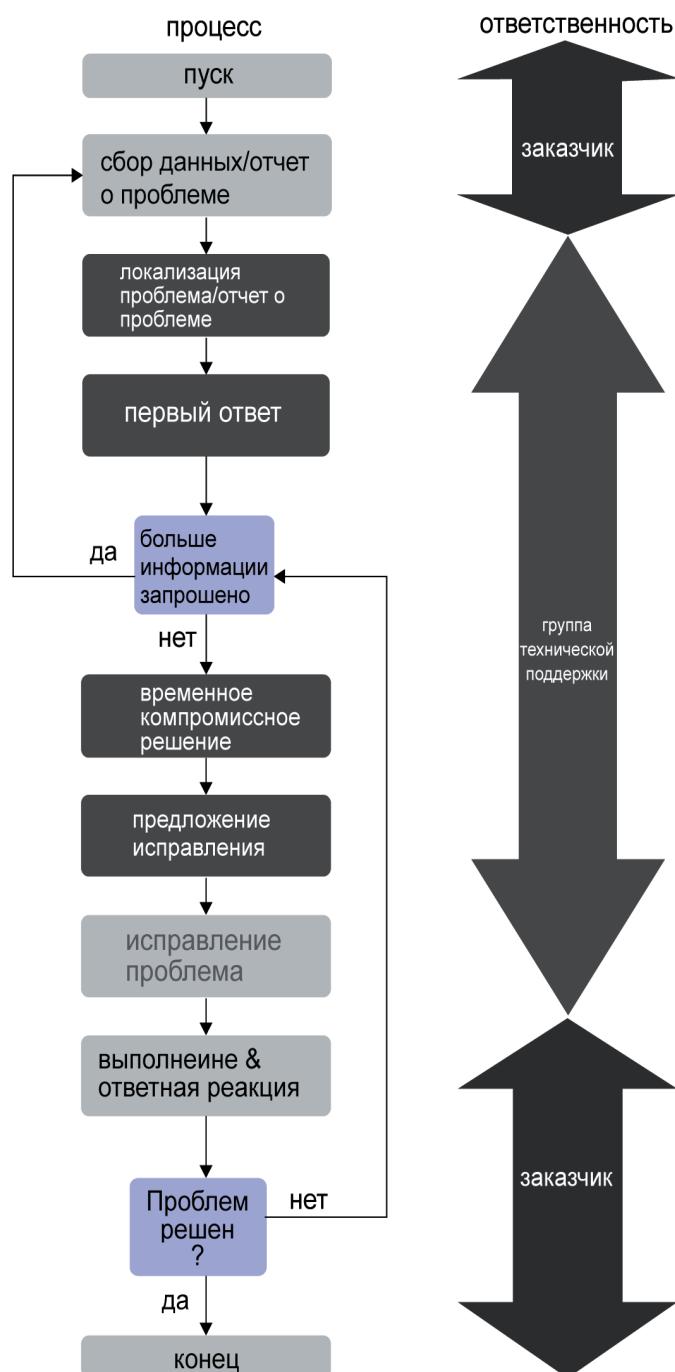
При поступлении сообщения об ошибке, требующей вмешательства оператора, регистрируется Отчет об ошибке (IR – incident report) и отмечается порядок ее срочности. Меры по устранению зарегистрированной ошибки проводятся в указанный срок согласно присвоенному порядку срочности. Группа поддержки FinFisher™ несет ответственность за координацию расследования и принятие решения по Отчету об ошибке, и сообщение отправителю IR о текущем статусе и обновленной информации.

При вопросах высокой важности мы обеспечиваем бесперебойную работу системы посредством оперативного предоставления решений нейтрализации отказов и проверенных инструкций устранения ошибок. Когда группа поддержки FinFisher™ предоставляет решение нейтрализации отказа, она одновременно передает Отчет о проблеме (PR – problem report) в отдел исследований и разработок (R&D – Research & Development) с целью обеспечения срочного решения. Такие профессиональные мероприятия технической поддержки гарантируют соответствие качества программного обеспечения самым высоким требованиям.

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

FIN SUPPORT

На схеме, приведенной ниже, показана стандартная последовательность выполнения работ и соответствующие ответственные подразделения.  
(Примечание: на данной схеме, под словом "заказчик" имеется ввиду отправитель IR):



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FIN SUPPORT**

В Таблице внизу приведена стандартная последовательность обработки ошибки, требующей вмешательства оператора:

<b>Заказчик</b>	<b>Обработка Отчета об ошибке (IR) и задачи</b>
	FinFisher™ имеют специально отведенный адрес э-почты, номера горячей линии телефона/факса для регистрации ошибок, требующих вмешательства оператора.
В случаях (предполагаемых) дефектов программного или аппаратного обеспечения, Отчет об ошибках (IR) поступает согласно определенному методу сообщения.  IR должен включать следующее: - идентификационный номер контракта - имя заказчика - поврежденная система / устройство - описание повреждения - уровень приоритетности (смотри определение ниже) - наличие симптомов ошибки	
Заказчик участвует в решении проблемы посредством предоставления подробных симптомов ошибки по запросу	Не позднее одного рабочего дня, Заказчик получает присвоенный номер зарегистрированному уведомлению, что подтверждает получение и прослеживает Отчет об ошибке, включая результаты предварительного анализа
	FinLifelineSupport поддерживают процесс сбора симптомов ошибок, по запросу
	FinLifelineSupport помогают в разработке временных решений по нейтрализации отказов
	FinLifelineSupport предоставляют предложения по корректировке проблем, включенных в Отчет об ошибках, что включает плановые корректирующие мероприятия и время для ответных действий/реагирования, после проведения анализа случившегося отказа
	FinLifelineSupport обеспечивают выпуск модификаций программного или аппаратного обеспечения, если зарегистрированный случай требует исправлений
Заказчик выполняет предоставленные модификации программного/аппаратного обеспечения. Заказчик подтверждает успешность выполнения исправлений.	FinLifelineSupport оказывают поддержку в выполнении модификации аппаратного(i)/ программного обеспечения

(i) В случае отсутствия гарантии, оплата за аппаратное обеспечение насчитывается отдельно.



# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FIN SUPPORT**

## Определения приоритетности вопросов и ошибок

FinLifelineSupport обрабатывают входящие отчеты вопросов и проблем согласно их уровню срочности. Уровень срочности определяют по двум факторам, оба из которых включаются в каждый Отчет IR:

- “Приоритетность”, основанная только на технических масштабах ошибки
- “Критичность ошибки для Заказчика” – является более объективным фактором и основывается на возможных последствиях ошибки для Заказчика

Таблица уровней приоритетности, приведенная ниже, дает общее представление о соответствующих технических масштабах ошибки:

Уровень	Определение	Пример
1	Критическая проблема: основной узел системы не работает	Сервер-посредник вышел из строя; невозможна установка связи с объектом FinSpy.
2	Большая проблема без временного решения	Антивирусное обновление обнаружило уже установленную RMS, что требует немедленного обновления, чтобы оставаться работоспособной в инфицированной системе.
3	Большая проблема с временным решением	Функции объекта FinSpy не работают надлежащим образом, но могут быть восстановлены на основании временного решения.
4	Небольшая проблема, оказывающая незначительное влияние на систему	Показывается неправильная иконка для загруженного файла

## Время реагирования

В 90 процентах всех случаев, мы выдерживаем время реагирования как показано в Таблице ниже.

“Рабочий день (дни)” = согласно определениям в немецком календаре, что исключает национальные праздники в Германии.

Время реагирования состоит из трех стадий:

- Предварительный ответ
- Комментарии Клиента относительно исправительных мероприятий
- Решение проблемы (или снижение уровня ее приоритетности)

Отчет времени на “Предварительный ответ” начинается с момента регистрации случая ошибки до фактического подтверждения отправки ответа Заказчику, подтверждающего получение сообщения об ошибке.

При “Предварительном ответе” может также быть запрошена дополнительная информация или, в менее сложных случаях, сразу отправлено решение проблемы.

# СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА И ЗАРАЖЕНИЯ

**FIN SUPPORT**

Время реагирования	Предварительный ответ	Комментарии Клиента относительно исправительных мероприятий	Решение ПРОБЛЕМЫ / Снижение уровня ПРИОРИТЕТНОСТИ
Уровень 1 – Критическая проблема	Тот же самый рабочий день	1 рабочий день	2 рабочих дня Примечание: В зависимости от проблемы и необходимости проведения исследований, решение проблемы может занять более продолжительное время.
Уровень 2 - Большая проблема без временного решения	Тот же самый рабочий день	2 рабочих дня	5 рабочих дней Примечание: В зависимости от проблемы и необходимости проведения исследований, решение проблемы может занять более продолжительное время.
Уровень 3 - Большая проблема с временным решением	Тот же самый рабочий день	3 рабочих дня	14 рабочих дней Примечание: В зависимости от проблемы и необходимости проведения исследований, решение проблемы может занять более продолжительное время.
Уровень 4 - Небольшая проблема	Тот же самый рабочий день	7 рабочих дней	7 рабочих дней

## ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Поддержка FinLifelineSupport включает регулярные обновления программного обеспечения и гарантирует автоматическое обновление существующей системы посредством корректировок к программному обеспечению, предоставляемых через обновление системы.

Такие обновления включают новые характеристики, расширение функциональных возможностей согласно стратегическому плану Заказчика (исключая аппаратное обеспечение).

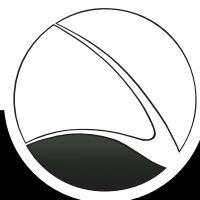


# ПРОГРАММА ИНСТРУКТАЖА ПО ИТ ПРОНИКОВЕНИЮ

## ОБУЧЕНИЕ FINTRAINING



Программа инструктажа по ИТ проникновению включает в себя курсы по инструктажу и по предоставляемым продукциям и практическому применению технологий ИТ проникновения. Данная программа передает многолетний опыт и знания конечным пользователям, таким образом, максимально увеличивая их возможности в этой сфере.



**FINFISHER™**  
IT INTRUSION

# ПРОГРАММА ИНСТРУКТАЖА ПО ИТ ПРОНИКНОВЕНИЮ

FINTRAINING

Знание и понимание мер безопасности **необходимы любому правительству** для того, чтобы поддерживать ИТ безопасность и успешно **предотвращать угрозы** ИТ инфраструктур, которые могут привести к потерям конфиденциальности, сохранности и доступности данных.

С другой стороны, такие темы, как **кибернетическая война**, активный перехват и сбор разведывательной информации путем **ИТ проникновения** стали более важными и актуальными, что требует, чтобы правительства **создавали команды по ИТ проникновению, которые могут решать такие задачи**.

Курсы инструктажа «FinTraining» проводят **специалисты мирового класса по ИТ проникновению в полностью практических условиях**, фокусирующих внимание на реальных операциях, как того требуют конечные пользователи для решения их **повседневных задач**.

КРАТКАЯ ИНФОРМАЦИЯ	
Применение:	Передача знаний
Возможности:	Ноу-ху по ИТ проникновению Возможности по кибернетической войне
Содержание:	Инструктаж

Gamma совмещает индивидуальные учебные занятия с **профессиональной и консультативной программами**, которые увеличивают или расширяют возможности команды по ИТ проникновению. Курсы инструктажа **полностью составляются по заказу клиента**, в зависимости от его операционных задач и требований.

**Операционная поддержка во время проведения программы предоставлена в стране клиента** для того, чтобы обеспечить извлечение наибольшей пользы из переданного ноухоу.

## Примеры тем на курсах инструктажа

- **Профилирование** объектов (веб-сайтов как и людей)
- Прослеживание **анонимных электронных писем**
- **Дистанционный доступ** к веб-почте
- **Оценка безопасности** по веб-серверам и услугам Интернета
- Практическое **использование слабостей программного обеспечения**
- **ИТ проникновение по беспроводным сетям** (WLAN/802.11 и Bluetooth)
- Атаки **критических инфраструктур**
- **Перехват данных и учетных данных пользователей** по сетям
- **Мониторинг точек доступа**, Интернет-кафе и гостиничных сетей
- **Перехват и запись звонков** (VoIP и DECT)
- **Взлом парольных хэш**

## Программа консультаций

- Полная программа инструктажа **ИТ проникновения и консультации**
- Структурированное создание и **обучение команды по ИТ проникновению**
- Полная **оценка членов команды**
- Практические учебные занятия, сфокусированные **на реальных операциях**
- **Консультация** в стране клиента

Пожалуйста, смотрите полный перечень функций в спецификации продукции



**FINFISHER™**  
IT INTRUSION



**WWW.GAMMAGROUP.COM**

GAMMA INTERNATIONAL  
United Kingdom

Tel: +44 - 1264 - 332 411  
Fax: +44 - 1264 - 332 422

[info@gammagroup.com](mailto:info@gammagroup.com)