

GROUP-IB
FORENSIC LAB:
КОМПЬЮТЕРНАЯ
КРИМИНАЛИСТИКА
И ИССЛЕДОВАНИЯ
ВРЕДОНОСНОГО
КОДА

Настоящий документ был подготовлен Group-IB исключительно в информационных целях и содержит только краткие справочные данные о продуктах и услугах компании. Настоящий каталог не является офертой, равно как и коммерческим предложением в какой-либо форме. Более подробную информацию о продуктах и услугах компании можно получить, обратившись к представителям Group-IB. Любое распространение документа или его части допускается лишь с письменного разрешения Group-IB. При цитировании документа ссылка на источник заимствования обязательна.

ВВЕДЕНИЕ

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА	3
ЛАБОРАТОРИЯ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ GROUP-IB	4
КАРТА УСЛУГ	5

ОПИСАНИЕ УСЛУГ

СБОР ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ	7
УЧАСТИЕ СПЕЦИАЛИСТОВ В ОРМ	9
КРИМИНАЛИСТИЧЕСКИЕ ИССЛЕДОВАНИЯ	11
ВОССТАНОВЛЕНИЕ ДАННЫХ	13
АУДИТ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	14
ИССЛЕДОВАНИЕ ВРЕДОНОСНЫХ ПРОГРАММ	15
РЕЦЕНЗИРОВАНИЕ СТОРОННИХ ЗАКЛЮЧЕНИЙ	17

О КОМПАНИИ

GROUP-IB	19
LETA GROUP	21

ВВЕДЕНИЕ

- КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА
- КАРТА УСЛУГ
- ЛАБОРАТОРИЯ КОМПЬЮТЕРНОЙ
КРИМИНАЛИСТИКИ И ИССЛЕДОВАНИЯ
ВРЕДОНОСНОГО КОДА GROUP-IB

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Компьютерная криминалистика является одним из ключевых направлений расследования компьютерных преступлений. В ходе своей работы криминалисты анализируют максимум данных, что позволяет им установить причины и хронологию инцидента, разобраться в методах и целях осуществления атаки, а также указать на причастных лиц. Поэтому заключение эксперта-криминалиста является основанием для возбуждения уголовного дела и служит важнейшим источником информации для последующего расследования.

Во время анализа цифровых носителей информации криминалисты восстанавливают хронологию событий; анализируют журналы файловой системы, операционной системы, приложений; изучают ключи реестра операционной системы; исследуют носитель на наличие вредоносного программного обеспечения. Также следует выделить особое направление в рамках компьютерной криминалистики – вирусную аналитику, нацеленную на изучение функционала, сетевых взаимодействий и алгоритма работы вредоносных программ.

Таким образом, в рамках криминалистических исследований компьютерной информации решаются следующие вопросы:

- ▶ о наличии признаков несанкционированного доступа к информационной системе, ее криптографическим компонентам;
- ▶ о наличии информации в явном, скрытом, удаленном или зашифрованном видах;
- ▶ о наличии вредоносного программного обеспечения, следов его работы и источников заражения;
- ▶ о хронологии событий в информационной системе, имеющих отношение к инциденту информационной безопасности;
- ▶ о неизменности (целостности) компьютерной информации после изъятия или исследования;
- ▶ иные экспертные вопросы.

Сегодня в России существует ограниченное количество специализированных криминалистических организаций, которые могут не только провести комплексную экспертизу носителей компьютерной информации, но и выполнить ее в соответствии с установленными требованиями законодательства.

Одним из наиболее квалифицированных отечественных центров является Лаборатория компьютерной криминалистики и исследования вредоносного кода, существующая на базе компании Group-IB, которая является единственной негосударственной организацией, предоставляющей услуги расследования компьютерных преступлений.

ЛАБОРАТОРИЯ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ И ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО КОДА GROUP-IB

Лаборатория компьютерной криминалистики и исследования вредоносного кода является специализированным подразделением компании Group-IB, занимающимся проведением экспертных исследований в области информационных технологий и компьютерной криминалистики, а также восстановлением данных с различных носителей информации.

В штате Лаборатории работает коллектив высококвалифицированных специалистов, обладающих соответствующим профильным образованием. Их опыт и знания подтверждены сертификатами международных криминалистических организаций. Кроме того, часть экспертов являются бывшими сотрудниками правоохранительных органов и обладают необходимым допуском для проведения компьютерных экспертиз.

Особо стоит отметить, что в рамках нашей Лаборатории функционирует подразделение вирусных аналитиков. Данные специалисты регулярно проводят изучение самых защищенных вредоносных программ, в том числе тех, которые на момент исследования не детектируются антивирусными средствами. Подобный тандем из компьютерных криминалистов и вирусных аналитиков позволяет проводить полные и исчерпывающие исследования самых сложных инцидентов, например таких, как мошенничество в системах интернет-банкинга, совершенных с применением вредоносных программ.

Помимо высококвалифицированных кадров, наша Лаборатория обладает новейшим экспертным оборудованием и программным обеспечением, позволяющим проводить компьютерные экспертизы любой сложности, в том числе по исследованию алгоритма работы вредоносного программного обеспечения и выявлению его функционала.

При производстве экспертиз используются:

- ▶ TABLEAU T3458is Forensics Bridge, аппаратный блокиратор записи;
- ▶ PC-3000 Flash SSD Edition, программно-аппаратный комплекс для восстановления данных с FLASH-накопителей и SSD;
- ▶ PC-3000 for Windows (UDMA), комплекс для диагностики и ремонта HDD ATA (SATA);
- ▶ AccessData Forensics toolkit Client, The Sleuth Kit и SANS SIFT Workstation, специализированные программные комплексы для криминалистического исследования;
- ▶ иное оборудование и программное обеспечение.

Благодаря совокупности перечисленных факторов за 2010 и 2011 годы криминалистами Group-IB было проведено более 400 исследований и экспертиз, из которых около 100 — для различных правоохранительных органов Российской Федерации, в том числе ФСБ России, МВД России и Следственного комитета РФ.

Заключения экспертов Group-IB по результатам проведения компьютерной экспертизы и криминалистических исследований соответствуют всем требованиям законодательства РФ и гарантированно принимаются в судах России.

За проведенные исследования и экспертизы сотрудники Лаборатории компьютерной криминалистики и исследования вредоносного кода неоднократно были отмечены благодарственными письмами как от коммерческих организаций, так и от различных подразделений правоохранительных органов, что подтверждает высокое качество проведенных работ.

КАРТА УСЛУГ

Криминалисты Group-IB оказывают следующие услуги:

- ▶ сбор доказательств в форме компьютерной информации и их юридически значимое оформление по факту инцидента информационной безопасности;
- ▶ участие в оперативно-разыскных мероприятиях и следственных действиях в качестве специалистов с целью обнаружения, идентификации и изъятия машинных носителей информации;
- ▶ криминалистические исследования (**в том числе по постановлениям правоохранительных органов и судов**) машинных носителей информации с целью ответа на поставленные вопросы;
- ▶ восстановление данных, в том числе и в рамках проводимых криминалистических исследований;
- ▶ аудит программного обеспечения с целью выявления присутствия вредоносного программного обеспечения или использования нелегальных программ;
- ▶ исследование вредоносного программного обеспечения с целью определения его алгоритма работы, функционала и совершаемых сетевых взаимодействий;
- ▶ рецензирование заключений экспертов и специалистов других организаций, в том числе и в рамках уголовных дел.

ОПИСАНИЕ УСЛУГ

- › СБОР ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ
- › УЧАСТИЕ СПЕЦИАЛИСТОВ В ОРМ
- › КРИМИНАЛИСТИЧЕСКИЕ ИССЛЕДОВАНИЯ
- › ВОССТАНОВЛЕНИЕ ДАННЫХ
- › АУДИТ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
- › ИССЛЕДОВАНИЕ ВРЕДОНОСНЫХ ПРОГРАММ
- › РЕЦЕНЗИРОВАНИЕ СТОРОННИХ ЗАКЛЮЧЕНИЙ

СБОР ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

ОПИСАНИЕ

Сбор доказательств в форме компьютерной информации проводится с целью юридически значимого и криминалистически правильного изъятия машинных носителей информации, а также копирования данных для дальнейшего исследования. Эта услуга необходима для анализа инцидента информационной безопасности с возможным последующим возбуждением и расследованием уголовного дела.

Специалисты Group-IB выполняют следующий спектр работ, связанных с корректным сбором цифровых доказательств:

- ▶ Предварительная консультация.
- ▶ Оперативный выезд специалиста на место инцидента.
- ▶ Сбор информации об инциденте и определение источников хранения доказательной информации по инциденту.
- ▶ Сбор имеющихся доказательств в виде компьютерной информации, их сохранение и оформление в соответствии с нормами законодательства РФ.
- ▶ Оформление необходимых документов.
- ▶ Консультирование уполномоченного представителя о мерах, необходимых для остановки инцидента и снижения ущерба.

Для обеспечения юридической значимости информации эксперты Group-IB выполняют ее сбор с учетом всех требований законодательства РФ, а также применяют неразрушающие методы копирования информации из информационных систем. Собранные данные и оригиналы носителей информации опечатываются способом, обеспечивающим невозможность доступа к информации без нарушения целостности упаковки, и скрепляются печатью организации заказчика и криминалиста Group-IB, а также подписями других лиц, участвующих в процессе. При этом все действия по сбору информации фиксируются в соответствующем протоколе, который затем подписывается всеми участниками процесса.

РЕЗУЛЬТАТ

В ходе сбора цифровых доказательств экспертом-криминалистом осуществляется идентификация машинных носителей информации, имеющих отношение к инциденту, их изъятие с последующим копированием данных.

В результате выполненных работ заказчику передаются:

- ▶ Опечатанные машинные носители информации, которые можно приобщить к уголовному делу в качестве доказательств.
- ▶ Скопированные криминалистически значимые данные, которые можно использовать для проведения внутреннего расследования инцидента информационной безопасности.
- ▶ Комплект документов, подтверждающих факты изъятия машинных носителей информации и копирования данных.

По итогам сбора цифровых доказательств заказчик может направить опечатанные машинные носители информации и скопированные данные в Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB для последующего криминалистического исследования. Данная услуга обеспечивает детальный анализ инцидента и является неотъемлемой частью его расследования.

ПРЕИМУЩЕСТВА

Корректный сбор цифровых доказательств в соответствии с существующими юридическими нормами является необходимой мерой при расследовании инцидентов информационной безопасности.

В результате оказания нашими экспертами услуги по сбору доказательств в форме компьютерной информации вы получите:

- ▶ **Корректно оформленные материалы.** Собранные в ходе мероприятия носители информации и данные оформляются в соответствии со всеми требованиями существующего законодательства. Это гарантирует, что полученная доказательная база будет рассмотрена и принята как правоохранительными, так и судебными органами.
- ▶ **Полный объем информации по инциденту.** Копирование данных производится из всех источников криминалистически значимой информации, что позволяет восстановить обстоятельства инцидента вне зависимости от любых попыток злоумышленника скрыть следы своих действий.
- ▶ **Независимость и достоверность полученных данных.** Достоверный результат, полученный в ходе сбора цифровых доказательств, обеспечивается полнотой и точностью выявления обстоятельств инцидента. Привлечение независимых специалистов обеспечит вам достоверность данных даже в тех случаях, когда в инцидент вовлечены внутренние сотрудники.
- ▶ **Возможность проведения криминалистического исследования.** В составе Group-IB работает Лаборатория компьютерной криминалистики и исследования вредоносного кода, куда можно направить собранные материалы для независимого комплексного исследования. Этот шаг позволит вам получить исчерпывающую информацию о произошедшем инциденте. Заключение эксперта-криминалиста принимается правоохранительными органами и судебными инстанциями в качестве допустимого доказательства при проведении гражданского, административного и уголовного производства.

УЧАСТИЕ СПЕЦИАЛИСТОВ В ОРМ

(Данная услуга предназначена только для правоохранительных органов)

ОПИСАНИЕ

В ходе подготовки и проведения оперативных или следственных мероприятий сотрудники правоохранительных органов сталкиваются с необходимостью сбора и исследования компьютерной информации. Цель услуги – привлечение высококвалифицированных экспертов Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB для содействия обнаружению, идентификации и изъятию материалов и документов, интересующих правоохранительные органы.

Специалисты Group-IB выполняют следующий спектр работ, связанных с участием в оперативно-разыскных мероприятиях:

- ▶ Консультирование сотрудников правоохранительных органов по вопросам обнаружения, идентификации и изъятия машинных носителей информации в конкретной ситуации.
- ▶ Выезд специалиста на мероприятие, проводимое правоохранительными органами.
- ▶ Содействие в обнаружении, идентификации и изъятии машинных носителей информации и документов, имеющих отношение к проводимым мероприятиям.
- ▶ Поиск компьютерной информации в соответствии с указанными характеристиками.
- ▶ Копирование криминалистически значимой компьютерной информации из источников, которые по каким-либо причинам не могут быть изъяты.
- ▶ Содействие в идентификации и опросе лиц, которые могут располагать сведениями, имеющих отношение к делу.
- ▶ Помощь в составлении протокола (по вопросам, требующим специальных знаний).

В рамках проводимых работ специалист производит следующие действия:

- ▶ Обнаружение, идентификация, отключение, упаковка и опечатывание машинных носителей информации.
- ▶ Копирование содержимого энергозависимых носителей информации (оперативной памяти) на машинный носитель информации специалиста.
- ▶ Копирование сетевого трафика на машинный носитель информации специалиста.
- ▶ Выявление документов, интересующих правоохранительные органы, на машинных носителях информации по заданным критериям (ключевым словам).
- ▶ Идентификация установленного на электронные вычислительные машины программного обеспечения.
- ▶ Иные.

Наши специалисты регулярно привлекаются к участию в оперативных и следственных мероприятиях, осуществляемых сотрудниками правоохранительных органов и прокуратуры, для содействия в идентификации, выемке и анализе доказательств в виде компьютерной информации. Все специалисты Group-IB, которые участвуют в оперативном реагировании на инциденты, проведении компьютерно-технических экспертиз и других криминалистических исследований, обладают необходимой квалификацией и опытом работы для соответствия статусу специалиста в соответствии с требованиями законодательства РФ.

РЕЗУЛЬТАТ

На все мероприятия криминалисты Group-IB выезжают оснащенные необходимым комплектом оборудования и программного обеспечения, что позволяет быстро и качественно решать любые поставленные задачи. В итоге сотрудникам правоохранительных органов передаются изъятые материалы и документы, которые можно приобщить к уголовному делу в качестве доказательств.

Следующим шагом для обеспечения доказательной базы, может быть передача объектов, изъятых в ходе оперативно-разыскных мероприятий, в Лабораторию компьютерной криминалистики и исследования вредоносного кода Group-IB. Материалы направляются на основании определения о назначении исследования в рамках ОРД или судебной компьютерно-технической экспертизы с указанием вопросов для разрешения в ходе выполнения работ.

ПРЕИМУЩЕСТВА

Корректный сбор компьютерной информации в соответствии с существующими юридическими нормами является необходимой мерой при проведении оперативно-разыскных мероприятий и следственных действий.

Результатом участия наших экспертов в мероприятиях, проводимых правоохранительными органами, являются:

- ▶ **Корректно оформленные материалы.** Собранные в ходе мероприятий носители информации и данные оформляются в соответствии со всеми требованиями существующего законодательства. Это гарантирует, что полученная доказательная база будет рассмотрена и принята в качестве допустимого доказательства судебными органами.
- ▶ **Полный объем информации по заданным характеристикам.** Копирование данных производится из всех источников криминалистически значимой информации, что позволяет получить максимальный объем вне зависимости от любых попыток сторонних лиц сокрыть следы своих действий.
- ▶ **Независимость и достоверность полученных данных.** Достоверный результат, полученный в ходе проводимых мероприятий, обеспечивается полнотой и точностью выявления обстоятельств по заданным параметрам. Привлечение независимых специалистов обеспечит достоверность данных при дальнейшем разборе обстоятельств дела.
- ▶ **Возможность проведения криминалистического исследования.** В составе Group-IB работает Лаборатория компьютерной криминалистики и исследования вредоносного кода, куда можно направить собранные материалы для независимого комплексного исследования. Этот позволит получить исчерпывающую информацию об изъятых данных. Заключение эксперта-криминалиста принимается судебными инстанциями в качестве допустимого доказательства при проведении гражданского, административного и уголовного производства.

КРИМИНАЛИСТИЧЕСКИЕ ИССЛЕДОВАНИЯ

ОПИСАНИЕ

Проведение криминалистического исследования является важной частью расследования инцидента информационной безопасности. Это связано с тем, что носители информации содержат сведения, которые могут пролить свет на произошедший инцидент, а также помочь в идентификации лиц, причастных к его совершению. Благодаря полученной информации заключение о проведенном криминалистическом исследовании может быть использовано в качестве доказательства. Однако такое заключение должно быть составлено независимым компетентным специалистом с использованием криминалистически верных методик и инструментов.

Криминалистическое исследование компьютерной информации и средств вычислительной техники проводится на основании:

- ▶ Постановлений о назначении судебных экспертиз от правоохранительных органов и судов.
- ▶ Запросов правоохранительных органов.
- ▶ Договоров с физическими и юридическими лицами.

Специалисты Group-IB выполняют следующий спектр работ, связанных с проведением криминалистических исследований:

- ▶ Восстановление хронологии каких-либо событий в информационной системе.
- ▶ Поиск следов предположительно несанкционированного доступа.
- ▶ Извлечение и анализ переписки (электронная почта, программы мгновенного обмена сообщениями).
- ▶ Поисковые задачи по заданным критериям.
- ▶ Криминалистическое исследование мобильных устройств.
- ▶ Исследование баз данных.
- ▶ Исследование скимминговых устройств.
- ▶ Исследование дампов сетевого трафика, дампов ОЗУ.
- ▶ Поиск вредоносного программного обеспечения, присутствующего на компьютере.
- ▶ Исследование содержимого криптоконтейнеров.
- ▶ Сравнение программных продуктов на предмет плагиата.
- ▶ Установление целостности (неизменности) содержимого машинных носителей информации после их изъятия.

Все криминалистические исследования, включая судебные экспертизы, проводятся в соответствии с требованиями российского законодательства с учетом методических рекомендаций ведущих государственных экспертных учреждений страны и международных организаций и принимаются в качестве допустимых доказательств в российских и иностранных судах.

РЕЗУЛЬТАТ

По итогам проведенных криминалистических исследований заказчиком передаются документы, содержащие обоснованные ответы на поставленные вопросы и иные сведения, имеющие отношение к делу.

Результаты криминалистического исследования компьютерной информации и средств вычислительной техники оформляются в виде:

- ▶ Заключение специалиста (для исследований, проводимых на основании запросов правоохранительных органов и договоров с юридическими и физическими лицами)
- ▶ Заключение эксперта (для исследований, проводимых на основании постановлений о назначении судебных экспертиз от судов и правоохранительных органов)

Заключения криминалистов Group-IB могут быть использованы как основания для возбуждения уголовного дела, так и для приобщения в качестве доказательств к уже возбужденному уголовному делу. Также результаты криминалистического исследования можно передать в Отдел расследований Group-IB для проведения расследования инцидентов информационной безопасности.

ПРЕИМУЩЕСТВА

Криминалистические исследования машинных носителей информации является основой для комплексного расследования инцидентов информационной безопасности и компьютерных преступлений. При этом цена ошибки на данном этапе крайне высока. Поэтому доверять проведение соответствующего исследования нужно только высококлассным специалистам, обладающим необходимой компетенцией и обеспечением.

В результате оказания нашими экспертами услуги по проведению криминалистических исследований вы получите:

- ▶ **Точность выводов.** Исследование компьютерной информации осуществляется криминалистически правильными методами, которые позволяют говорить о высоком уровне достоверности полученных результатов. Это достигается использованием аппаратных и программных блокираторов записи, а также исследованием копий содержимого машинных носителей информации.
- ▶ **Полноту выводов.** Все материалы, переданные в Лабораторию Group-IB, проходят комплексное и всестороннее исследование. Мероприятия проводятся на основе последних отечественных и зарубежных разработок в области компьютерной криминалистики, что подтверждает научную обоснованность полученных выводов.
- ▶ **Оперативность получения результата.** Благодаря обширным компетенциям криминалистов Group-IB и новейшему криминалистическому оборудованию все исследования проводятся в сроки, оговоренные при передаче материалов на анализ.
- ▶ **Юридическую значимость заключений.** Заключения экспертов и специалистов оформляются исключительно в соответствии с требованиями действующего законодательства и не содержат ошибок процессуального характера. Это позволяет гарантировать, что они будут приняты правоохранительными органами и судебными инстанциями в качестве допустимых доказательств при проведении гражданского, административного и уголовного производства.

ВОССТАНОВЛЕНИЕ ДАННЫХ

ОПИСАНИЕ

Утрата важной информации и ее недоступность через цифровые носители могут быть как случайностью — результатом поломки, брака, некорректного обращения, так и преднамеренным шагом со стороны злоумышленников с целью уничтожить определенные данные, в том числе «цифровые улики» преступления. Цель данной услуги — восстановление удаленных или поврежденных данных, записанных на различных типах носителей информации (накопители на жестких магнитных дисках, флеш-накопители, иные).

Специалисты Group-IB выполняют следующий спектр работ, связанных с восстановлением данных:

- ▶ Консультация специалистов по вопросам восстановления данных.
- ▶ Восстановление удаленных файлов различного типа (документы, фотографии, видеофайлы и т. п.).
- ▶ Восстановление данных после работы компьютерных вирусов.
- ▶ Восстановление данных после логического повреждения файловых систем.
- ▶ Восстановление данных, хранящихся на неисправных машинных носителях информации.
- ▶ Восстановление файлов, поврежденных в результате программной ошибки.

Криминалисты Лаборатории восстанавливают данные со всех применяемых носителей информации:

- ▶ НЖМД различных форм-факторов.
- ▶ Твердотельных накопителей.
- ▶ Flash-носителей
- ▶ RAID (отказоустойчивые массивы)
- ▶ Карт памяти
- ▶ Мобильных телефонов и смартфонов
- ▶ Планшетов, мультимедиа-устройств и др.

Все работы производятся на основании заключенного договора и в соответствии с соглашением о неразглашении конфиденциальной информации. Перед непосредственным выполнением работ по восстановлению информации производится бесплатная диагностика устройства, на основании которой специалист оценивает стоимость работ, а также возможность и объем восстановления данных.

РЕЗУЛЬТАТ

По итогам проведенной работы заказчику предоставляются восстановленные файлы, записанные на носитель информации заказчика либо на носитель информации, предоставляемый компанией Group-IB. Обладая самым современным и высококлассным оборудованием для работы с носителями информации, специалисты Group-IB могут не только восстановить данные, но и провести исследование и дать соответствующее заключение (о причине выхода из строя носителя информации, о файлах, содержащихся на нем), предоставить полный отчет о проделанной работе.

АУДИТ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ОПИСАНИЕ

Использование нелицензионного программного обеспечения распространено в российских компаниях. Руководители зачастую не догадываются, какого рода программы установлены на компьютерах. Тем самым не учитываются риски, связанные с нарушением существующего законодательства: проверка компьютеров организации правоохранными органами может обернуться солидным штрафом. Кроме того внутри информационной сети компании может быть широко распространено вредоносное программное обеспечение, работа которого может привести к плачевным результатам.

Group-IB предлагает услугу по проведению аудита программного обеспечения, установленного на компьютерах компании заказчика. Цель данной услуги: составление списка программ, работающих на компьютерах в организации, с учетом различных требований, оценка последствий их работы и минимизация рисков.

Специалисты Group-IB выполняют следующий спектр работ, связанных с аудитом программного обеспечения:

- ▶ Составление списка программ, присутствующих на компьютерах заказчика.
- ▶ Выявление вредоносных программ, устранение их и следов их работы, составление рекомендации по противодействию им.
- ▶ Выявление технических особенностей установленных программ, которые могут выступать в качестве «признаков контрафактности».
- ▶ Анализ лицензионных договоров, заключенных между заказчиком и правообладателями. Выявление нарушений положений лицензионных договоров.
- ▶ Выявление программ, запрещенных к использованию в соответствии с политикой информационной безопасности организации.

Аудит программного обеспечения производится без нарушения работы информационной системы заказчика. Сделано это будет с максимальным комфортом для заказчика в любое удобное для него время и с наименьшим вмешательством в работу компании. Аудит осуществляется на основании соглашения о неразглашении конфиденциальной информации (NDA), что гарантирует нашим клиентам полную конфиденциальность.

РЕЗУЛЬТАТ

По итогам проведенного аудита заказчик получает отчет, содержащий:

- ▶ Список программ, присутствующих на компьютерах заказчика.
- ▶ Обстоятельства установки обнаруженных программ (дата и время установки, использованный дистрибутив).
- ▶ Технические особенности установленных программ, которые могут выступать в качестве «признаков контрафактности».
- ▶ Технические характеристики обнаруженных вредоносных программ.
- ▶ Список нарушений условий лицензионных договоров и рекомендации по их устранению.
- ▶ Рекомендации по устранению выявленных нарушений.

Данное заключение может быть использовано как для удаления нежелательного программного обеспечения, что обеспечит информационную безопасность компании, так и для оспаривания необоснованно принятых правоохранными и надзирающими органами решений об использовании нелицензионных программ. Также отдельно могут быть предоставлены рекомендации по противодействию использованию контрафакта и составлен возможный список альтернативных программ, бесплатных или наиболее дешевых.

ИССЛЕДОВАНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

ОПИСАНИЕ

Вредоносное программное обеспечение является неотъемлемой частью преступлений в сфере высоких технологий. Современные программы, используемые злоумышленниками, способны выполнять различные задачи, начиная от неправомерного копирования конфиденциальной информации и заканчивая организацией удаленного управления персональным компьютером.

Для комплексного расследования инцидента, в котором применялось вредоносное программное обеспечение, необходимо исследование предположительно вредоносных программ с целью установления их алгоритма, функционала и осуществляемых сетевых взаимодействий.

Специалисты Group-IB выполняют следующий спектр работ, связанных с исследованием программ:

- ▶ Определение алгоритма вредоносной программы.
- ▶ Извлечение из вредоносной программы списка управляющих серверов.
- ▶ Документирование функциональных особенностей вредоносной программы (например, особенностей ее взаимодействия с системами дистанционного банковского обслуживания).
- ▶ Определение и документирование реализованных в программе способов противодействия криминалистическому исследованию и обнаружению.
- ▶ Документирование изменений, вносимых программой в системный реестр и файловую систему в целом.
- ▶ Определение и описание иных действий программы с информацией, которые могут иметь значение для уголовного дела.
- ▶ Исследование конфигурационных файлов и дополнительных программных модулей, загружаемых вредоносной программой из сети Интернет (при необходимости).
- ▶ Корреляция полученной информации с другими экземплярами вредоносных программ.

Исследование вредоносного программного обеспечения производится как в виде независимого исследования, так и в виде судебной компьютерно-технической экспертизы. Все криминалистические исследования, включая судебные экспертизы, проводятся в соответствии с требованиями российского законодательства с учетом методических рекомендаций ведущих государственных экспертных учреждений страны и международных организаций и принимаются в качестве допустимых доказательств в российских и иностранных судах.

РЕЗУЛЬТАТ

По итогам исследования заказчик получает заключение специалиста, оформленное с учетом требований действующего законодательства, содержащее:

- ▶ Описание алгоритма вредоносной программы, ее функциональных особенностей, а также осуществляемых программой сетевых взаимодействий.
- ▶ Описание дополнительных программных модулей и конфигурационных файлов, загружаемых из сети интернет.

- ▶ Рекомендации по использованию полученных сведений в целях расследования инцидента информационной безопасности.

Заключения криминалистов Group-IB могут быть использованы для приобщения в качестве доказательств к уголовному делу. Также результаты криминалистического исследования можно передать в Отдел расследований Group-IB для проведения расследования инцидентов информационной безопасности.

РЕЦЕНЗИРОВАНИЕ СТОРОННИХ ЗАКЛЮЧЕНИЙ

ОПИСАНИЕ

Сегодня как в России, так и за рубежом существуют организации, предлагающие услуги компьютерной криминалистики. К сожалению, не все из них обладают соответствующими высокопрофессиональными экспертами или необходимым оборудованием. Часто отчеты о проведенных ими исследованиях не соответствуют нормам законодательства, поэтому рискуют быть непринятыми правоохранительными органами и судебными инстанциями. В связи с этим мы предлагаем услуги рецензирования заключений сторонних экспертов с целью анализа научной обоснованности, полноты и всесторонности проведенных ими криминалистических исследований.

Специалисты Group-IB выполняют следующий спектр работ, связанных с рецензированием заключений:

- ▶ Выявление технических и процессуальных ошибок в заключениях экспертов и специалистов (включая ошибки в назначении судебной экспертизы, ошибки в постановке вопросов эксперту и т. п.).
- ▶ Оценка научной обоснованности и допустимости использованных методик криминалистического исследования компьютерной информации.

Анализ предоставленных заключений производится с точки зрения существующих криминалистических требований к исследованию компьютерной информации, методик исследования компьютерной информации и требований к оформлению заключений экспертов. Оформление всех обнаруженных ошибок и неточностей осуществляется в виде заключения специалиста, которое может быть приобщено к уголовному делу и использовано в качестве доказательства в суде.

РЕЗУЛЬТАТ

По итогам проведенного рецензирования заказчик получает заключение специалиста, содержащее:

- ▶ Список технических и процессуальных ошибок и неточностей в предоставленном заключении эксперта или специалиста.
- ▶ Обоснованную оценку полноты и всесторонности проведенного криминалистического исследования.
- ▶ Результаты анализа научной обоснованности использованных методик исследования компьютерной информации.

Заключение специалиста выполняется с учетом всех требований действующего законодательства и может быть приобщено к уголовному делу и использовано в качестве доказательства в суде.

О КОМПАНИИ

- GROUP-IB
- LETA GROUP

GROUP-IB

Основанная в 2003 году компания Group-IB является единственной в России коммерческой организацией, которая оказывает полный комплекс услуг по расследованию инцидентов информационной безопасности и компьютерных преступлений. Входит в состав LETA Group.

Group-IB оказывает следующий спектр услуг в сфере расследований компьютерных преступлений и информационной безопасности:

- ▶ Реагирование на инциденты в круглосуточном режиме.
- ▶ Расследование компьютерных преступлений, в том числе мошенничеств в системах интернет-банкинга.
- ▶ Предотвращение DDoS-атак.
- ▶ Выявление и блокирование фишинговых сайтов.
- ▶ Выявление в сети интернет информации об организациях, против которых готовятся либо совершались кибератаки.
- ▶ Компьютерно-технические экспертизы электронных носителей информации и электронно-вычислительных машин.
- ▶ Идентификация и анализ вредоносного программного обеспечения с целью определения его алгоритма, функционала и совершаемых сетевых взаимодействий.
- ▶ Восстановление данных с любых электронных носителей информации.
- ▶ Правовое сопровождение вопросов, связанных с использованием информационных технологий и расследованием компьютерных преступлений.
- ▶ Комплексный и специализированный аудит информационной безопасности.

Group-IB – единственная компания, которая предлагает услуги обеспечения информационной безопасности в режиме «24x7x365».

На базе Group-IB осуществляет свою деятельность CERT-GIB, круглосуточный центр быстрого реагирования на инциденты информационной безопасности. Миссией данной структуры является осуществление сбора данных об инцидентах, а также координация ответных мероприятий, направленных на снижение финансового и репутационного ущерба.

КОМПЕТЕНЦИИ

Group-IB предоставляет заказчикам не только уникальный состав, но и уровень сервиса. Высокие показатели работы компании достигаются за счет:

- ▶ профессионализма и компетентности сотрудников, подтвержденных международными сертификатами в области информационной безопасности и компьютерной криминалистики;
- ▶ уникальной базы знаний, накопленной за многолетнюю практику реагирования и расследования;
- ▶ собственных криминалистической и антивирусной лабораторий;
- ▶ профессионального дорогостоящего оборудования и экспертного уровня его применения;

- ▶ наличия собственно распределенной сети специальных программно-аппаратных комплексов Honey Net, направленные на отслеживание действий компьютерных злоумышленников и методов совершения преступлений;
- ▶ продолжительной и эффективной совместной работы с правоохранительными органами различных государств;
- ▶ сотрудничества с различными независимыми организациями по расследованию киберпреступлений в 52 странах мира, что обеспечивает оперативное получение необходимой информации по инцидентам, совершенным международными группами компьютерных преступников;
- ▶ партнерств с производителями уникального программного и программно-аппаратного обеспечения в области информационной безопасности и компьютерной криминалистики.

Все работы проводятся в соответствии с законодательством Российской Федерации на базе опыта международных организаций по расследованию ИТ-инцидентов, борьбе с компьютерной преступностью и кибертерроризмом.

Заключения экспертов Group-IB по результатам проведения расследований, компьютерно-технической экспертизы и криминалистических исследований соответствуют всем требованиям законодательства РФ и гарантированно принимаются в судах России.

Специалисты Group-IB постоянно проходят обучение по новейшим методикам расследования ИТ-инцидентов и борьбе с киберпреступностью, вовлечены в регулярный процесс обмена опытом и рекомендациями с мировым профессиональным сообществом.

LETA GROUP

LETA Group — управляющая компания в сфере передовых информационных технологий. Основной задачей Группы компаний LETA является обеспечение успешного развития и совместного функционирования компаний, входящих в состав группы.

Стратегическая задача LETA Group: создание и развитие лидеров в выбранных областях деятельности, открытие новых путей продвижения бизнеса.

LETA Group — консолидатор инновационных идей в сфере информационных технологий.

В структуре LETA Group существует четыре дивизиона, в рамках которых осуществляется деятельность компании:

- ▶ **LETA Group Information Security** — информационная безопасность от защиты домашнего компьютера до защиты государственных и корпоративных ИТ-систем. Компании Дивизиона: LETA IT-company, Group-IB, ESS Distribution.
- ▶ **LETA Group Industrial Innovation** — информационные технологии и индустриальные инновации в промышленности. Компании Дивизиона: ASK Labs, АСКОМ-строй.
- ▶ **LETA Group Software Development** — создание корпоративного и «домашнего» программного обеспечения. Компании Дивизиона: ДАМАК, HamsterSoft.
- ▶ **LETA Group Investment&Venture** — инвестиции в передовые ИТ-проекты.



Основанная в 2003 году, компания Group-IB является первой в России и в странах СНГ компанией, профессионально и комплексно занимающейся расследованием обстоятельств компьютерных преступлений и нарушений информационной безопасности. В составе Group-IB работает Лаборатория компьютерной криминалистики, оказывающая услуги независимой компьютерно-технической экспертизы, в том числе правоохранительным органам Российской Федерации.
Входит в Leta Group.

107023, Москва,
Мажоров переулок, д. 14, стр. 2.
Тел.: +7 (495) 661-55-38
E-mail: info@group-ib.ru
www.group-ib.ru