



Эффективное реагирование на инциденты и расследование компьютерных преступлений

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

При цитировании документа ссылка на источник заимствования обязательна.



Оглавление

Вступление	4
Карта услуг.....	6
Уникальные конкурентные преимущества.....	8

Описания услуг

Расследование инцидентов ИБ

Реагирование на инциденты ИБ.....	11
Расследование инцидентов ИБ.....	14
Программы сопровождения и поддержки.....	17
Юридическое сопровождение дел по расследованию инцидентов.....	19
Защита от DDoS.....	20
Антифрод (предотвращение мошенничества в системах ДБО).....	22

Компьютерная криминалистика

Услуги лаборатории компьютерной криминалистики.....	25
Восстановление данных.....	27
Безопасный бренд.....	29
Ответы на наиболее частые вопросы (основные заблуждения).....	32

О компаниях

LETA IT-company.....	35
Group-IB.....	37
LETA Group.....	39



Вступление

Предложение LETA IT-company и Group-IB направлено на обеспечение баланса превентивных и сдерживающих мер для достижения экономической эффективности и сбалансированности мер защиты

Регулярно на современном рынке компании подвергаются кибератакам. С ростом уровня информатизации бизнеса многократно увеличивается уровень возможных финансовых потерь и рисков, а для киберпреступников растет привлекательность получения противозаконного заработка.

Активный рост преступлений в сфере информационных технологий приходится именно на Россию. Ключевым фактором стремительной эволюции и развития преступности в области высоких технологий является слабая юридическая база в сфере квалификации действий и преследования хакеров в правовом поле. Это приводит к ощущению безнаказанности для «виртуальных» мошенников. Из-за неразвитой правоприменительной практики в области расследования преступлений ИБ такие инциденты зачастую предпочитают скрывать, что дополнительно стимулирует активность киберпреступников.

Сегодня в России расследование киберпреступлений затруднено. Этому способствует и новизна сферы, и специфичность состава преступлений, и малочисленный состав подразделений органов внутренних дел, ответственных за расследования, а также ряд других факторов. В то же время суммы финансовых потерь увеличиваются. Например, убытки от противоправных действий киберпреступников в рамках дистанционного банковского обслуживания клиентов в среднем для одного банка составляют более 10 млн руб. в год.

В сложившихся условиях российский рынок невольно становится центром развития киберпреступности. По экспертным оценкам, к концу 2010 года количество активно действующих хакеров составило около 20 тысяч, а объем выручки в сфере киберкриминала достигло \$1 млрд в год. При этом ответственность за свои действия в среднем несут только 5 – 7 преступников, что не составляет даже 0,1% от общего количества киберпреступлений. Это в свою очередь является фактором роста числа новых противоправных действий.

При этом «гонка вооружений», которую ведут компании, действующие в России, закупая в целях защиты от новых угроз все больше ИБ-решений, постепенно теряет эффективность. Предусмотреть все информационные риски невозможно, а растущий парк оборудования и программного обеспечения нужно постоянно поддерживать. Стоимость владения и управления инфраструктурой неуклонно растет, что ведет к неоправданным издержкам.

Наиболее эффективным решением для бизнеса на сегодня является комплексная защита, обеспечивающая баланс превентивных и сдерживающих мер, позволяющий обеспечить экономию и максимальную отдачу от вложения средств. Время только экстенсивной защиты постепенно приходит к концу. Для получения конкурентных преимуществ необходимо не только защищаться, но и эффективно реагировать на инциденты информационной безопасности. Зачастую, обеспечив качественное и эффективное реагирование и управление инцидентами, организация может получить выгоды, а не ущерб.

Расследование инцидентов ИБ – уникальная для России услуга, предоставляемая LETA IT-сотрапу совместно с компанией Group-IB. Услуга обеспечивает организации, подвергшейся несанкционированному воздействию на информационные активы, неотвратимость ответственности злоумышленников за совершенные правонарушения и высокую вероятность возмещения ущерба, тем самым существенно снижая финансовые и репутационные риски.

Карта услуг

Пакет предложений LETA IT-company и Group-IB в области ИБ-инцидентов включает в себя расследование и предотвращение случаев:

- неправомерного доступа к компьютерной информации (в том числе атак и действий хакеров);
- создания, использования и распространения вредоносного программного обеспечения;
- возникновения корпоративных ИТ-инцидентов;
- появления мошенничеств в сетях связи;
- покушений на права и свободы граждан, связанных с информационными технологиями
- и т.д.

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

Реагирование на инциденты ИБ

- Оперативный выезд специалиста 24 x 7.
- Компьютерно-техническая (криминалистическая) экспертиза:
 - восстановление хронологии событий;
 - анализ журналов файловой системы, операционной системы, приложений;
 - изучение ключей реестра операционной системы;
 - исследование носителя (-ей) на наличие вредоносного программного обеспечения;
 - полный анализ вредоносного программного обеспечения;
 - восстановление удаленной информации;
 - поиск и изучение информации на носителе в соответствии с запросом заказчика;
 - оформление отчета.

- Сбор доказательной базы.
- Выявление причин возникновения инцидента.
- Разработка и предоставление рекомендаций по минимизации рисков.
- Юридическое оформление всех отчетов и проведение работ в правовом поле.
- Консультации по эффективности и целесообразности проведения правового расследования для принятия решения о дальнейших мероприятиях.

Расследование инцидентов ИБ

- Проведение работ по выявлению информации, позволяющей идентифицировать злоумышленников.
- Сбор и оформление документов для передачи в правоохранительные органы.
- Сопровождение и поддержка на этапе следственных мероприятий.
- Сопровождение и поддержка на этапе судебного процесса.
- Полное юридическое сопровождение дел по расследованию инцидентов в области ИБ.

Сопутствующие услуги

- Организация процесса управления инцидентами.
- Аудит настроек электронных сервисов и систем с целью минимизации рисков отсутствия информации, необходимой для эффективного расследования инцидента.
- Правовая оценка документов (договоры ДБО; документы, регламентирующие режим конфиденциальности, и т.п.).
- Инструментальная проверка на наличие уязвимостей сервисов и систем.
- Тестирование уязвимостей от лица потенциального злоумышленника («тесты на проникновение»).
- Защита от распределенных атак «отказ в обслуживании» DDoS.
- Мониторинг незаконного использования бренда в сети Интернет, защита от фишинга.
- Восстановление удаленной информации.
- Расшифровка зашифрованных данных.
- Обучение персонала.

Уникальные конкурентные преимущества

LETA IT-company и Group-IB предлагают первый и единственный на российском рынке комплекс услуг по расследованию инцидентов ИБ

Быстрое реагирование

- Молниеносное реагирование:
 - режим SOS! – блокирование инцидента сразу после обнаружения (например, отражение DDoS-атаки в течение 30 – 60 минут с момента поступления звонка);
 - приезд эксперта-криминалиста в течение 60 минут после вызова.
- Круглосуточный режим работы (24 x 7 x 365):
 - все удобные заказчику каналы связи: стационарный и мобильный телефон, электронная почта, интернет-пейджеры.

Международное сотрудничество

- Мировой охват и масштаб деятельности – отлаженные партнерства с организациями, занимающимися расследованием компьютерных преступлений, и государственными силовыми структурами в 43 странах мира:
 - ускоренное расследование международных инцидентов – до 30 раз быстрее (взаимодействие с участием зарубежных инстанций в течение 1 – 3 дней в отличие от «официальных» 2 – 3 месяцев);
 - наработанные алгоритмы международного взаимодействия при расследовании киберпреступлений с зарубежными «следами».

Специальные средства

- Профессиональное и дорогостоящее оборудование:
 - современные мобильные и стационарные полнофункциональные криминалистические лаборатории;
 - применение специализированных высокоточных систем стоимостью до \$500 тыс.

Индивидуальный бизнес-ориентированный подход

- Индивидуальное выстраивание состава услуги (и, соответственно, стоимости) по принципу «конструктора».

Контроль сотрудников, прозрачность взаимодействия

- Наличие подразделения собственной безопасности (не осуществляющего взаимодействия с заказчиками), осуществляющего проверки сотрудников и целостности собранной информации.
- Использование специализированных технических средств, обеспечивающих контроль целостности информации, собранной в качестве доказательной базы.
- Возможность физического присутствия специалистов заказчика на всех стадиях реагирования, сбора информации и расследования инцидента.
- Соглашение о неразглашении информации.
- Соглашение об уровне сервиса.
- Все взаимоотношения регулируются договорными отношениями.

Опыт и уникальные методики, нарабатываемые с 2003 года

- Уникальный опыт и компетенции:
 - обученные специалисты с навыками работы на специализированном оборудовании;
 - знание процессов и процедур сбора, оформления, предоставления доказательств (включая «цифровые») в правовые и судебные инстанции;
 - тонкое знание законодательных норм, применяемых в области ИБ;
 - наработанные связи с инстанциями, участвующими в проведении расследований (ФСБ, отдел «К», прокуратура, суды);
 - сильное «ИБ-окружение» (наряду с Group-IB в состав LETA Group входят LETA IT-company, обеспечивающая полный спектр услуг в области построения ИБ в организации, компания ESET, обладающая собственной вирусной лабораторией, а также другие компании);
 - обширная накопленная база знаний.

Специалисты LETA IT-company и Group-IB в течение многих лет специализируются на вопросах информационной безопасности и постоянно проходят обучение по новейшим методикам расследования ИТ-инцидентов и методам противодействия киберпреступности, а также используют лучшие практики и технические средства для обеспечения конфиденциальности работ и коммуникаций с клиентами.

Все работы проводятся в соответствии с законодательством Российской Федерации. За основу берется опыт международных организаций по расследованию ИТ-инцидентов, борьбе с компьютерной преступностью и кибертерроризмом.

Описание услуг

**Расследование
инцидентов ИБ**

Реагирование на инциденты

Проблематика

Ежедневно инциденты, связанные с информационной безопасностью, происходят в организациях по всему миру. Не существует 100%-ной защиты, всегда остаются риски, которые могут быть реализованы случайно или намеренно. Профиль рисков для каждой организации уникален. При этом многие риски не рассматриваются совсем либо механизмы их снижения не соответствуют их уровню. Это потенциально ставит организацию перед возможными негативными событиями, такими как кража ценной информации, утечка персональных данных, нарушение работоспособности интернет-ресурсов, причинение предприятию ущерба репутации и др.

В основном инциденты, представляющие риск для организации и требующие немедленного реагирования, можно разделить на внутренние (например, утечка конфиденциальных данных, аномальная сетевая активность, компрометация информации и т.д.) и внешние (например, DDoS-атаки, фишинг, попытки взлома и сканирования портала и т.д.). Перечень инцидентов чрезвычайно широк.

Состав услуги

Услуга по оперативному реагированию на инциденты включает:

- немедленную консультацию сертифицированных специалистов;
- оперативную разработку и помощь в реализации плана реагирования на инцидент с учетом мировых практик управления инцидентами ИБ и особенностей организации заказчика;
- оперативное устранение критичных уязвимостей;
- разработку рекомендаций по улучшению мер защиты информации;
- разработку плана и набор рекомендаций по расследованию инцидента;

- оперативное предоставление информации по первоначальным этапам расследования и рекомендаций по оперативному восстановлению бизнес-процессов;
- предоставление полного списка необходимых действий для полного восстановления после инцидента;
- предоставление полного отчета, включающего информацию о проделанной работе;
- собрание участвующих в совместной работе лиц для обсуждения проделанной работы по устранению инцидента и прояснения всех деталей.

Чтобы свести к минимуму ущерб от инцидента, команда оперативного реагирования LETA IT-company и Group-IB оказывает необходимую поддержку немедленно.

В кратчайшие сроки заказчику предоставляется максимально полная информация о произошедшем инциденте и путях его локализации независимо от того, была ли это атака на сайт, систему банковского обслуживания, программное обеспечение или любые другие информационные активы.

Подход к каждому инциденту индивидуален. В процессе реагирования разрабатывается оперативный план действий, нацеленный на скорейшее сдерживание инцидента, снижение ущерба и восстановление критичных бизнес-процессов.

Существующие альтернативы (традиционные способы решения)

Практика реагирования на инциденты ИБ только начинает формироваться. На сегодня разработчики ИБ- и ИТ-решений предлагают системы управления инцидентами. Однако одних только технических средств недостаточно. «Интеллектуальные» инциденты со стороны злоумышленников, учитывающие контур защиты заказчика, прошлый опыт неправомерного доступа к его информационным активам, могут быть предотвращены только «двойным» инструментарием – оборудованием и опытным экспертом, умеющим грамотно его настроить и квалифицированно применить. Альтернативы предложению LETA IT-company и Group-IB, равной ему по эффективности, на сегодняшний день не существует.

Выгоды

LETA IT-company и Group-IB первыми в России начали профессионально оказывать услуги по реагированию на инциденты информационной безопасности на коммерческой основе. Наши основные преимущества:

- мы готовы немедленно приступить к реагированию на инцидент: 24 часа в сутки, 7 дней в неделю;
- наши эксперты являются сертифицированными специалистами в области информационной безопасности и управления инцидентами, обладающими самым большим опытом в России;
- мы обладаем новейшим, уникальным в России оборудованием и методиками для проведения компьютерной криминалистической экспертизы;
- наша методика реагирования на инциденты полностью адаптирована к требованиям законодательства Российской Федерации;
- опыт реагирования и расследования инцидентов информационной безопасности позволяет предвидеть хронологию протекания инцидентов и осуществлять упреждающие меры по его сдерживанию и остановке.

Результатом работы LETA IT-company и Group-IB являются юридически правильно оформленные доказательства и отчеты, что позволяет использовать их в судебных разбирательствах

У группы реагирования LETA IT-company и Group-IB есть опыт управления инцидентами в организациях различных размеров и сфер бизнеса, начиная с SMB и заканчивая ведущими мультинациональными компаниями. Тесное взаимодействие между группой реагирования и сотрудниками службы ИБ/ИТ заказчика позволяет быстро локализовать инцидент и организовать процесс по сбору доказательств и восстановлению инфраструктуры.

Расследование инцидентов ИБ

Проблематика

Системы защиты и контроля информации, установленные в организации, не исключают на 100% рисков несанкционированного воздействия злоумышленников на информационные активы. Если инцидент ИБ все-таки произошел, организации необходимо провести его грамотное расследование – выявить уязвимости, пресечь их дальнейшее использование, определить «источник» угрозы, ее исполнителя, грамотно собрать улики и доказательства преступления и предоставить материалы в правоохранительные органы для возбуждения дела об административном и (или) уголовном правонарушении.

ВАЖНО!

Доказательства, связанные с компьютерными преступлениями и изъятые с места происшествия, могут быть легко изменены как в результате ошибок при их изъятии, так и в процессе расследования. Представление подобных доказательств в судебном процессе требует специальных знаний и соответствующей подготовки.

Для выполнения подобных задач необходимы отдельные человеческие ресурсы и их 100%-ное вовлечение в процесс. При этом необходима высокая квалификация специалистов – владение методиками и процедурами сбора и представления доказательств, их подачи в компетентные инстанции, знание законодательных нормативов и тонкостей для формирования понятного состава обвинения (в условиях работы со случаями нарушения законодательства в узкоспециализированной сфере, которая обычно недостаточно понятна представителям судебно-административной системы) и т.д.

Состав услуги

LETA IT-company и Group-IB выполняют весь спектр работ, связанных с расследованием нарушений информационной безопасности:

- восстановление хронометража событий;
- выявление причин произошедшего инцидента;
- выявление лиц, причастных к инциденту;
- оказание информационной поддержки для предотвращения и профилактики инцидентов;
- юридическое сопровождение:
 - анализ организационно-распорядительной документации, определяющей режим коммерческой тайны;

- анализ договоров, регламентирующих отношения субъектов бизнес-деятельности (ДБО);
- консультации по формированию комплекта документов для возбуждения уголовного или административного дела;
- сопровождение, консультационная поддержка процесса на этапе следственных мероприятий;
- оформление информации (доказательств) в качестве юридически значимой доказательной базы;
- представление интересов в гражданском судопроизводстве;
- представление интересов в арбитражном судопроизводстве.

Услуга расследования инцидентов ИБ включает комплекс услуг по раскрытию киберпреступлений (предотвращение, обнаружение, реагирование и расследование инцидентов ИБ) и законодательному преследованию злоумышленников в сфере компьютерных технологий.

Существующие альтернативы (традиционные способы решения)

На российском рынке практика расследования киберпреступлений с прозрачной системой ответственности, которую бы в обязательном порядке несли правонарушители, не имеет широкой юридической практики. У служб безопасности организаций, как правило, не хватает ресурсов, а иногда и квалификации. Ответственные за расследования ведомства занимают достаточно пассивную позицию в отношении возбуждения и ведения уголовных дел. В связи с этим организации-жертвы, как правило, стараются замалчивать случаи кибератак. Во многом это связано с рядом неясностей по сбору и представлению доказательств. В итоге понесенные финансовые и имиджевые потери не возмещаются.

Выгоды

Расследование инцидентов ИБ обеспечивает неизбежную ответственность преступников и законное востребование возмещения причиненных убытков

- **Финансовая эффективность и экономия**
 - За цену, эквивалентную окладу одного опытного аудитора инцидентов ИБ, вы получаете команду с многолетним опытом, круглосуточно готовую среагировать на ваш вызов, а также систему обнаружения вторжений, обслуживаемую и обновляемую в круглосуточном режиме. Наши сотрудники сертифицированы различными организациями (в том числе ISACA, ACFE, IISFA) и строго придерживаются кодекса этики аудиторов инцидентов ИБ
 - Вам не нужно покупать дорогостоящее оборудование для проведения компьютерной экспертизы

- Возбуждение уголовного дела может быть необходимым атрибутом признания случая страховым и выплаты предусмотренной страховой компенсации
 - Предложение LETA IT-company и Group-IB позволяет не отрывать сотрудников от основной работы и не проводить их дорогостоящее обучение расследованиям компьютерных инцидентов
 - Вы получаете уникальные выгоды максимальной защищенности для клиентов организации (например, банка) и, соответственно, увеличение ее капитализации
 - Наши специалисты осуществляют юридическую проверку договоров на предмет возмещения убытков за инциденты
- **Защита и укрепление имиджа**
 - Создание в глазах киберпреступников образа «опасного» игрока, жестко отстаивающего свои интересы и «неудобного» для последующих кибернападений
 - Использование успешных расследований в качестве PR-акции
- **Повышение безопасности**
 - Постоянный контроль рисков ИБ, регулярное проведение оценки рисков ИБ
 - Снижение количества корпоративных рисков, связанных с инцидентами ИБ. Проведение расследований стимулирует осознание ответственности и последствий совершения компьютерного преступления
 - Наставничество, коучинг. LETA IT-company и Group-IB проводят обучение персонала применению принципов безопасной работы с ИС в повседневной работе, а также оперативному реагированию на инциденты, повышая его осведомленность в вопросах обеспечения ИБ
- **Стандартизованность и корректность процедур**
 - Соответствие российским судебно-правовым нормативам. Обладая необходимым экспертным опытом и знаниями специфики деятельности по расследованию инцидентов ИБ, LETA IT-company и Group-IB проводят оформление доказательств для судебного разбирательства в соответствии с нормами законодательства РФ, ведь неправильный сбор улик или их оформление – это козырь обвиняемого в компьютерном преступлении
 - Соответствие международным стандартам. Расследование ИТ-инцидентов, как и аудит, проводится LETA IT-company и Group-IB с участием независимой третьей стороны – в соответствии с рекомендациями международных стандартов

Возбуждение уголовного дела в большинстве случаев может быть показателем серьезности намерений компании в отношении злоумышленников само по себе.

ВАЖНО!

В ряде случаев (например, в рамках дистанционного банковского обслуживания) допущенный инцидент помимо понесенных в результате инцидента финансовых потерь может привести к штрафным санкциям со стороны клиента организации. Услуга LETA IT-company и Group-IB обеспечивает заказчику скрупулезную юридическую проверку и доработку договоров с целью исключения таких рисков и четкой фиксации отсутствия финансовой ответственности.

Программы сопровождения и поддержки

Для удобства заказчиков LETA IT-company и Group-IB предлагают готовые комплексные пакеты услуг сопровождения и поддержки с ежемесячной оплатой, позволяющие максимально полно защититься от возможных киберугроз по принципу абонентской подписки.

Услуги	Программы поддержки		
	Standard	Primary	Premium
Реагирование на инциденты ИБ: · по телефону · через Интернет, службы мгновенных сообщений · доступность офиса 24/7 · оперативный выезд аудитора инцидентов в течение 1 часа с момента поступления заявки · сбор и анализ информации об инциденте · определение мер по минимизации ущерба и сдерживанию инцидента			
Расследование инцидентов и правовая поддержка: · сбор электронных доказательств для обращения в правоохранительные органы · расследование инцидента и проведение экспертизы · правовая поддержка по вопросам расследования инцидентов и компьютерных преступлений · взаимодействие с правоохранительными органами РФ и других стран			
Консультирование и внедрение: · консультирование по вопросам информационной безопасности · разработка политик и процедур реагирования на инциденты ИБ · обучение персонала процедурам реагирования на инциденты ИБ · определение настроек ИС для корректного сбора информации об инцидентах (журналы, отчеты, сообщения о тревоге)			

Мониторинг защищенности и аудит ИБ:

- защита одного ресурса от распределенных атак на отказ в обслуживании (DDoS-атаки)
- защита одного ресурса от фишинга и кражи интеллектуальной собственности – мониторинг сети Интернет на наличие сайтов-клонов
- обеспечение безопасности использования систем дистанционного банковского обслуживания (ДБО) «Банк-клиент», «Интернет-банкинг» и прочее
- 1 раз в 6 месяцев проведение анализа защищенности ключевых элементов ИТ-инфраструктуры (внешний периметр, внутренняя инфраструктура, веб-сайты и веб-приложения)
- 1 раз в 12 месяцев проведение полного аудита информационной безопасности, включающего:
 - анализ защищенности корпоративной сети
 - тестирование на проникновение
 - аудит процессов информационной безопасности

Аутсорсинг команды реагирования

На территории вашей организации или удаленно всегда находится минимум один специалист Group-IB по расследованию инцидентов, который обеспечивает:

- оперативные сервисы по реагированию на инциденты
- мониторинг систем обнаружения вторжений и журналов событий
- мониторинг и анализ защищенности корпоративной сети компании
- взаимодействие со всеми участниками процесса расследования инцидентов информационной безопасности – внутренними подразделениями заказчика, правоохранительными, силовыми органами и судебными инстанциями, правовыми экспертами, профессиональными ассоциациями

В рамках любого пакета услуги оперативного дежурства и поддержки оказываются круглосуточно – 7 дней в неделю, 365 дней в году.

Примеры расследуемых инцидентов

Внутренние

- Утечка конфиденциальной информации
- Неправомерный доступ к информации
- Удаление информации
- Компрометация информации
- Саботаж
- Мошенничество с помощью ИТ
- Аномальная сетевая активность
- Аномальное поведение бизнес-приложений
- Использование активов компании в личных целях или в мошеннических операциях

Внешние

- Атаки типа «Отказ в обслуживании» (DoS), в том числе распределенные (DDoS)
- Перехват и подмена трафика
- Фишинг
- Взлом, попытка взлома, сканирование портала компании
- Сканирование сети, попытка взлома сетевых узлов
- Вирусные атаки
- Неправомерный доступ к конфиденциальной информации
- Анонимные письма (письма с угрозами)
- Размещение конфиденциальной/провокационной информации на форумах и блогах

Юридическое сопровождение дел по расследованию инцидентов

Проблематика

С развитием информационных технологий в общественных отношениях появилась новая область, нуждающаяся в правовом регулировании. Сегодня практически любая деятельность человека связана с использованием ИТ, что обостряет актуальность вопросов законодательного регулирования компьютерных преступлений.

В настоящее время в России сформирован базис основных нормативных актов, в той или иной степени затрагивающих информационные технологии. Однако отдельные правовые нормы, касающиеся киберпреступности, рассредоточены в различных отраслях права и для эффективного применения против злоумышленников требуют глубоких знаний в области как права, так и компьютерных технологий.

Состав услуги

LETA IT-company и Group-IB предлагают заказчикам следующую юридическую помощь:

- консультирование по вопросам отношений, связанных с информационными технологиями (например, юридическая проверка договоров на предмет возмещения в пользу заказчика убытков, понесенных из-за инцидентов информационной безопасности);
- помощь в составлении заявлений с целью обращения в правоохранительные органы;
- помощь в составлении исковых заявлений;
- представление интересов в гражданском судопроизводстве;
- представление интересов в арбитражном судопроизводстве.

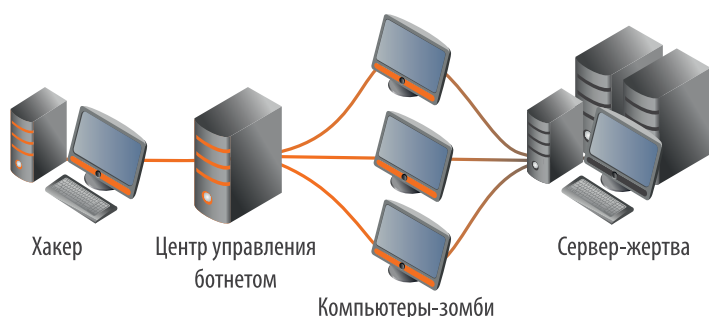
Грамотное использование правовых норм при применении ИТ обеспечивает заказчику легитимную и финансовую безопасность, а также обеспечивает дополнительные выгоды клиентам организации.

Защита от DDoS

Проблематика

Распределенная атака на отказ в обслуживании (DDoS) – это атака на сетевые ресурсы и сервисы с целью приостановления деятельности и затруднения доступа к ним.

Схема DDoS-атаки



Сложность и негативные последствия DDoS-атак постоянно возрастают. Если в 2005 году самая крупная зарегистрированная DDoS-атака составляла всего 3,5 Гбит/сек, то на сегодня объем передаваемых при проведении атаки данных увеличился до 80 Гбит/сек – мощности, достаточной атакующей стороне для воздействия даже на сети национального уровня.

Состав услуги

LETA IT-company и Group-IB обеспечивают комплексный подход к защите от DDoS – сочетание специализированного оборудования, программного обеспечения, выделенного канала для противодействия самым крупным атакам и опыта экспертов. Трафик заказчика пропускается через фильтрующую сеть и возвращается уже очищенным. Независимо от того, закончилась текущая атака или началась новая, ресурсы клиента не почувствуют никакой дополнительной нагрузки и будут всегда защищены.

Даже если вы еще не являетесь подписчиком одной из программ поддержки, а атака уже идет, LETA IT-company и Group-IB готовы начать подавление атаки немедленно.

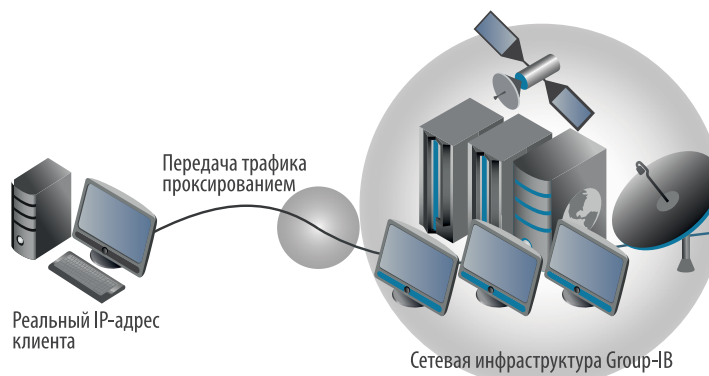
Точки присутствия LETA IT-company и Group-IB расположены по всему миру, что позволяет оперативно реагировать на атаку из любого региона и остановить ее прямо у источника. Доступ к фильтрующим системам в российских и зарубежных сетях дает LETA IT-company и Group-IB возможность:

- блокировать «паразитный» трафик, объемы которого ставят под угрозу магистральные каналы ведущих провайдеров;
- максимально удешевлять стоимость услуги для клиентов, столкнувшихся с атаками, превышающими даже 27-гигабитный порог.

Маршрутизация трафика осуществляется двумя основными путями (с учетом индивидуальных потребностей заказчика подходы могут изменяться и комбинироваться).

1. Переадресация DNS (прокси)

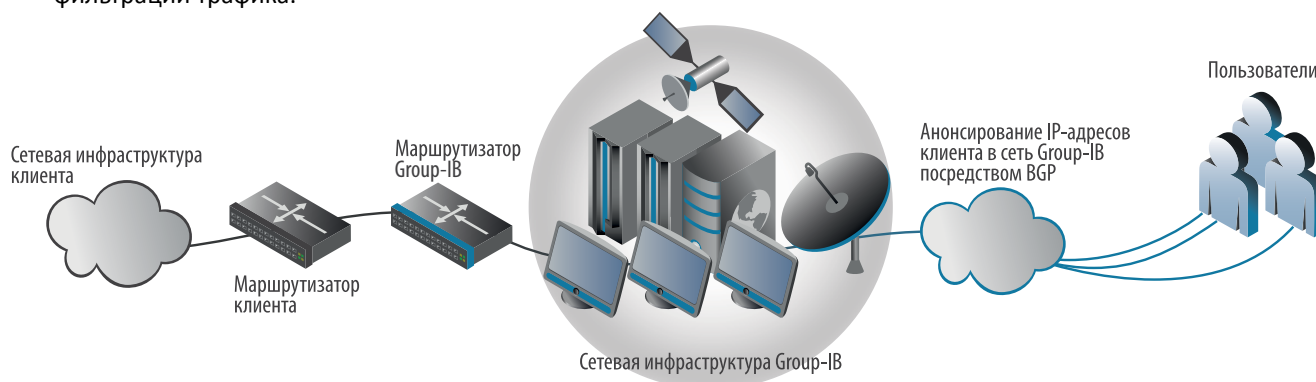
Заказчику предоставляется IP-адрес в защитной сети (IPN). Посредством изменения DNS весь трафик заказчика проходит через сетевую инфраструктуру LETA IT-company и Group-IB. После очищения от вредоносного контента трафик направляется обратно в сеть клиента. Это базовый метод, остающийся самым быстрым.



2. BGP-роутинг (протоколы GRE)

Клиентская подсеть и канал трафика переадресовываются в инфраструктуру LETA IT-company и Group-IB посредством протокола GRE, что предоставляет клиенту ряд преимуществ, включая полный контроль над процессом фильтрации трафика.

На практике подавление DDoS-атаки занимает от 1 до 24 часов в зависимости от масштаба и готовности специалистов заказчика оперативно изменить конфигурацию оборудования.



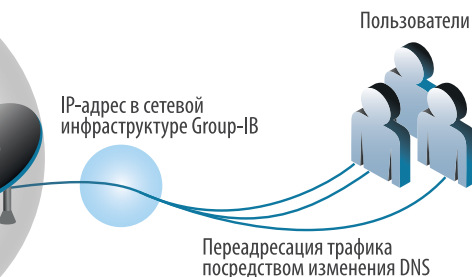
Процедура подключения услуги защиты от DDoS обычно занимает не более 2 часов (в зависимости от обновления базы DNS может очистить трафик заказчика в срок до 30 минут) и состоит из следующих трех шагов:

1. Обратитесь в Group-IB с запросом на подключение услуги.
2. Исходя из объема легитимного трафика (генерируемого в обычном режиме работы без учета атаки) дежурный сообщит вам стоимость защиты. Для немедленного подключения услуги достаточно отсканированного гарантийного письма об оплате.
3. Вам назовут IP-адрес, на который нужно перевести A-запись зоны DNS в настройках вашего хостинга. После смены A-записи в течение 1 – 4 часов (время зависит от обновления DNS-записей в сети Интернет) весь трафик будет перенаправлен через распределенную сеть LETA IT-company и Group-IB и выведен на сервер заказчика в очищенном от вредоносного контента виде.

Существующие альтернативы (традиционные способы решения)

Обычно для защиты от DDoS-атак используются специальные аппаратные решения – серверное и сетевое оборудование или «широкий» канал, предоставляемый далеко не всеми провайдерами. Эти решения слишком высоки в цене. Кроме того, существующие аппаратные средства эффективны против не более чем 80 типов стандартных DDoS-атак, осуществляемых через примитивные бот-сети. При этом против мощных «интеллектуальных» кибератак, учитывающих алгоритмы выстроенной системы защиты и обходящих ее, они бессильны.

LETA IT-company и Group-IB обеспечивают защиту от DDoS мощностью до 28 гигабит в секунду (мировой уровень) и без предоплаты.



Антифрод

(предотвращение мошенничеств в системах дистанционного банковского обслуживания – ДБО)

Проблематика

За последнее время системы «Банк-клиент» стали неотъемлемой частью взаимодействия коммерческих организаций с банками. Удобство применения таких систем трудно недооценить: они позволяют снизить издержки и повысить оперативность проведения финансовых операций.

Однако, по данным МВД, только в Москве каждый месяц происходит больше десятка успешных мошеннических операций с использованием систем дистанционного банковского обслуживания (ДБО): «Банк-клиенты», «Интернет-банкинг» и прочее. Средний ущерб по каждому инциденту составляет более 3 млн рублей. Помимо этого, ежедневно сотрудниками служб безопасности банков пресекаются попытки мошенничества на суммы в сотни миллионов рублей.

Кража денежных средств может быть произведена как сотрудниками организации, так и абсолютно не имеющими к ней отношения людьми. В большинстве случаев компрометация электронных ключей происходит с помощью вредоносного ПО, которое проникает через Интернет. Этот код обнаруживает, что на

данном ПК ведется работа с системой ДБО, и осуществляет копирование ключей и логина/пароля пользователя, а затем передает данную информацию злоумышленникам. Кроме того, возможны случаи, когда перевод денежных средств осуществляется непосредственно с ПК жертвы посредством ПО для удаленного администрирования, также установленного мошенниками через сеть Интернет.

Хранение ключей на жестком диске компьютера или незащищенном внешнем носителе (дискете, flash-диске) существенно упрощает получение несанкционированного доступа к ним. Как правило, компания узнает, что с ее счета были украдены денежные средства, уже после того, как деньги прошли через несколько счетов юридических и физических лиц и были успешно обналичены. При этом злоумышленники прикладывают все усилия к уничтожению доказательств своей преступной деятельности и препятствуют доступу компании-жертвы к счетам. Для этого используются различные способы вывода из строя персонального компьютера, с которого производилась кража ключей и логина/пароля пользователя. Также часто применяются DDoS-атаки на серверы банков и интернет-шлюзы компании-жертвы для затруднения доступа к счетам через систему ДБО.

Несмотря на сложные схемы мошенничеств, преступные группы в системах ДБО оставляют следы незаконной деятельности, по которым они могут быть идентифицированы и привлечены к ответственности.

Состав услуги

LETA IT-company и Group-IB предлагают полный спектр услуг, связанных с расследованием инцидентов информационной безопасности в ДБО:

- остановку инцидента и блокирование платежных поручений;
- юридически значимый сбор электронных доказательств по инциденту;
- исследование и юридически значимое оформление результатов исследования доказательств по инциденту;
- проведение компьютерно-технической экспертизы носителей информации;
- проведение аналитических работ по идентификации причастных к инциденту лиц и методов совершения инцидента;
- проведение анализа экземпляров вредоносного кода;
- расследование DDoS-атак;
- юридическое сопровождение материалов в правоохранительных органах и в суде;
- создание и реализацию плана по снижению рисков информационной безопасности;
- разработку и внедрение стандартов и политик по обеспечению информационной безопасности;
- абонентское обслуживание в рамках реагирования на инциденты, юридической поддержки, аудитов информационной безопасности и анализа рисков.

После поступления от заказчика звонка с сообщением об инциденте пропажи денежных средств с расчетного счета специалисты LETA IT-company и Group-IB максимально быстро приложат необходимые усилия, чтобы остановить платежные поручения и воспрепятствовать завершению мошеннической операции.

Электронные улики недолговечны и требуют особого бережного отношения в момент сбора и анализа, чтобы не уничтожить важные

для расследования данные и обеспечить их юридическую значимость.

***Правильный и своевременный
сбор улик – 50% успеха
расследования. Поэтому так
важен их оперативный сбор
компетентными специалистами.***

В ходе анализа инцидента выявляются причины и источники его происхождения. Анализ уязвимостей, которые позволили злоумышленникам – как внутренним, так и внешним – осуществить мошенничество, дает возможность выявить слабые места в организационных, технических и правовых методах защиты информации, применяемых заказчиком, создать и реализовать эффективный и оптимальный по затратам план по снижению рисков ИБ.

Существующие альтернативы (традиционные способы решения)

На сегодня подавляющее число организаций преимущественно способно предотвращать реализацию мошеннических операций, разрабатывая технические и поведенческие рекомендации для своих заказчиков. В силу непроработанной практики борьбы с киберпреступлениями расследование, уголовное преследование мошеннических действий на сегодня затруднено.

Выгоды

Антифрод-политика разрабатывается на основе уникальной базы знаний LETA IT-company и Group-IB, глубоко локализованной в соответствии с российской спецификой и превосходящей доступные в России, но не локализованные западные решения.

Описание услуг

**Компьютерная
криминалистика**

Услуги лаборатории компьютерной криминалистики

Проблематика

Современный бизнес высоко информатизирован. В таких условиях потребность в анализе, интерпретации, обработке «цифровой» доказательной базы является постоянной. Проведение этих работ требует сложного специального оборудования и высокой квалификации сотрудников.

Состав услуги

LETA IT-company и Group-IB проводят следующие типы компьютерно-криминалистических исследований и экспертиз по инцидентам информационной безопасности:

- исследование носителей информации с целью поиска, восстановления и оформления доказательств;
- экспертиза электронной переписки на предмет ее достоверности;
- исследование вредоносного программного обеспечения;
- восстановление зашифрованных, поврежденных данных с носителей информации;
- аудит ИТ-инфраструктуры на соответствие рекомендациям по протоколированию и журналированию;
- экспертиза программного обеспечения на соблюдение требований лицензирования и нарушения прав правообладателя;
- анализ достоверности содержания и происхождения электронных документов и цифровой информации;
- поиск и получение информации из зашифрованных документов и контейнеров;

- использование аппаратных средств блокирования записи (100%-ная гарантия сохранения оригинальных носителей);
- поиск необходимой информации в любых типах файлов, в том числе в изображениях и в удаленных данных;
- восстановление данных
- и др.

При проведении исследований и экспертиз LETA IT-company и Group-IB учитывают имеющуюся судебную практику и комментарии к кодексам РФ и к проводимым делам различных форматов.

Существующие альтернативы (традиционные способы решения)

Обычно сбор доказательств «цифрового» нарушения доверяют сотрудникам ИТ-подразделения организации. Между тем только специалисты, которые ежедневно участвуют в расследовании инцидентов, способны осуществлять компьютерные исследования и экспертизы наиболее качественно и профессионально.

Заключения экспертов лаборатории компьютерной криминалистики LETA IT-company и Group-IB принимаются как достаточные при проведении гражданского, административного и уголовного делопроизводства.

Восстановление данных

Проблематика

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 «стереть» невыгодные им данные или «цифровые» улики преступления. В обоих случаях организации, столкнувшейся с проблемой восстановления данных, необходимо ее оперативное и надежное решение.

Состав услуги

LETA IT-company и Group-IB оказывают следующие услуги:

- восстановление данных с поврежденных носителей;
- восстановление данных с USB-flash (флешки);
- восстановление данных после форматирования или удаления;
- восстановление данных с ноутбука;
- восстановление информации после переустановки ОС;
- восстановление информации с жесткого диска;
- восстановление данных с RAID;
- восстановление файлов и баз данных;
- восстановление данных с любых других носителей.

Существующие альтернативы (традиционные способы решения)

Как правило, у организаций нет штатных подразделений, специализирующихся на восстановлении данных. При подозрении на утрату информации организации или обращаются к ИТ-специалистам,

которым не всегда удастся выявить и решить специализированные проблемы, или вынуждены срочно заниматься поиском и выбором надежного подрядчика. В условиях высокой занятости, недостоверности рыночных предложений это затруднительно и часто несет угрозу стабильности работы организации.

Выгоды

Одним из ключевых преимуществ предложения LETA IT-company и Group-IB является комплексность предлагаемых услуг – восстановление утраченных данных в составе портфеля взаимоувязанных ИБ-сервисов.

Уникальная специализация LETA IT-company и Group-IB в области расследования инцидентов ИБ и расследований компьютерных преступлений обеспечивает высокое качество услуги. LETA IT-company и Group-IB обладают самым современным оборудованием для восстановления данных с любых носителей информации. Лаборатория компаний постоянно работает со сложными случаями восстановления данных при разнообразных инцидентах информационной безопасности. Среди заказчиков лаборатории – МВД РФ.

Обладая самым современным и высококласным оборудованием для работы с носителями информации, специалисты LETA IT-company и 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.

Безопасный бренд

Проблематика

С ведением коммерческой деятельности в Интернете связано огромное число рисков, игнорируя которые, предприятие может понести финансовые потери. Ежемесячно десятки компаний по всему миру подвергаются атакам мошенников. При этом падает репутация бренда и, соответственно, снижается прибыль. Ежегодно мошенники крадут со счетов банков огромные суммы.

Только заблаговременная подготовка к атаке и быстрое реагирование на нее могут помочь снизить убытки от действий злоумышленников.

Состав услуги

Предложение LETA IT-company и Group-IB позволяет в режиме реального времени обнаруживать угрозы неправомерного использования бренда в сети Интернет и противостоять им. Основной задачей услуги является обеспечение безопасного присутствия торговой марки заказчика в Интернете.

Решение LETA IT-company и Group-IB включает в себя комплекс услуг по мониторингу, защите и быстрому реагированию на атаки мошенников. Услуга включает:

- превентивную регистрацию доменов для защиты от киберсквоттинга¹;
- анти-фишинг и борьбу со злоупотреблением брендом;
- сбор и анализ информации об инциденте, расследование инцидента и проведение экспертизы;
- сбор электронных доказательств для обращения в правоохранительные органы;

¹ Киберсквоттинг — приобретение доменных имен, созвучных названиям известных компаний, или просто с «дорогими» названиями с целью их дальнейшей перепродажи или размещения рекламы (<http://ru.wikipedia.org/wiki/Cybersquatting>).

- взаимодействие с правоохранительными органами и командами по реагированию на инциденты мира, в том числе и Российской Федерации.

Безопасный бренд – это:

- гарантия надежности вложения инвестиций в маркетинг:
 - пресечение манипуляций с SEO,
 - защита от киберсквоттинга;
- быстрое обнаружение широкого спектра нарушений: мониторинг большого числа онлайн-источников данных – аукционов, B2B/B2C-обменников, сайтов электронной коммерции, социальных средств массовой информации, досок объявлений, электронной почты;
- защита доходов и прибыли: обнаружение и закрытие в правовом порядке сайтов торговли контрафактными товарами;
- защита от ложных ассоциаций на веб-сайтах и сайтах социальных сетей и тем самым защита от снижения репутации бренда;
- укрепление доверия к бренду за счет своевременного предупреждения клиентов заказчика о вредоносных сайтах еще до вступления в силу активных мер по борьбе с фальшивыми и опасными ресурсами.

Существующие альтернативы (традиционные способы решения)

В силу новизны киберпространства как нового «измерения» для ведения бизнеса на сегодня не выработаны системные меры по противодействию злоумышленникам, негативно влияющим на репутацию марки и стоимость бренда. Помимо этого, еще не сформировано законченное представление о полном, исчерпывающем спектре злонамеренных действий в киберсреде, способных нанести урон торговой марке заказчика.

Примеры угроз

- **Мошенничество.** Существует целая отрасль киберпреступности, направленная на обман через Интернет клиентов «жертвы». Уверены ли вы, что не существует сайт www.yourbrand2.com, который торгует контрафактной продукцией под видом вашей или просто продает несуществующий товар от вашего имени?
- **Фишинг.** Целью этого вида интернет-мошенничества является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Под вашей торговой маркой третьими лицами осуществляется фальсифицированная рассылка или создается поддельный интернет-ресурс, цель которых – вызвать доверие клиентов организации и стимулировать их для сообщения своих данных (логина, пароля, номера и кода пластиковой карты и т.д.). Действия злоумышленников направлены на кражу данных ваших клиентов и нанесение прямого репутационного и финансового ущерба.
- **Черный PR.** Мнимая анонимность Интернета породила новую волну маркетинговых войн. Часто со специально созданных ресурсов осуществляются подложные публикации от имени той или иной компании или ее высокопоставленного лица, которые оказывают влияние на общественность, целевую аудиторию организации (как правило, негативное) и наносят финансовый урон бизнесу.
- **Киберсквоттинг.** Приобретение доменных имен, созвучных названиям известных компаний (или просто «дорогих» названий с целью их дальнейшей перепродажи или размещения рекламы). Подход может использоваться для последующей организации фишинговых атак.

Выгоды

Услуга «Безопасный бренд» дает быструю отдачу при минимальных вложениях.

Приобретение услуги обеспечивает заказчику надежный контроль компетентными, опытными специалистами целого комплекса потенциальных «уязвимостей», способных воспрепятствовать бизнесу в современной киберсреде.

LETA IT-company и Group-IB имеют соглашения с ключевыми разработчиками браузеров – Internet Explorer и Opera. Это позволяет добиться быстрого попадания любого фишингового сайта, заявленного как опасного, в стоп-лист браузеров и оперативного снятия его угрозы для заказчиков.

Ответы на наиболее частые вопросы (основные заблуждения)

{Почему такое же расследование инцидента ИБ не может провести собственная ИБ-служба организации?}

Есть несколько основных причин, почему для проведения расследования организации не подойдут ресурсы собственной ИБ-службы и будут полезны услуги LETA IT-company и Group-IB:

1. Для выделения людей на расследование произошедшего инцидента, которое, как правило, непредсказуемо и требует срочного реагирования, у организации обычно нет необходимых человеческих ресурсов.
2. Расследование инцидента требует особой профессиональной подготовки, квалификации и опыта, которыми в подавляющем большинстве случаев не обладают штатные сотрудники службы ИБ.
3. Нередко инцидент ИБ происходит по инициативе, преднамеренному умыслу или вине сотрудника организации. В этом случае, участвуя в его расследовании на стороне предприятия, он будет вводить следствие в заблуждение и всячески мешать установлению истины, прикладывая усилия к уничтожению и искажению доказательств.

Ведение расследования третьей, независимой стороной снимает подобные риски.

{Услуга по расследованию инцидентов – «конкуренция» службе ИБ?}

Расследование инцидентов на сегодня – уникальный пакет услуг, аналогов которому нет в России. Кроме того, услуги компаний как третьей, независимой стороны в процессе подачи иска помогают заказчику с юридической точки зрения. Сотрудники подразделения ИБ заказчика получают в свое распоряжение квалифицированных сотрудников, которые в состоянии оказать эффективную и качественную поддержку при возникновении инцидентов, требующих безотлагательного решения. Общее управление и предоставление результатов реагирования и расследования для руководства осуществляется сотрудниками заказчика. Таким образом, Group-IB – это качественный инструмент в руках сотрудников ИБ, а конкуренции между мастером и инструментом быть не может.

{ Почему нам можно доверять реагирование и расследование инцидентов? }

Мы осуществляем контроль сотрудников исполнителей работ. Для этой цели создано подразделение собственной безопасности (не осуществляющее взаимодействие с заказчиками).

Использование специализированных технических средств, обеспечивающих контроль целостности информации, собранной в качестве доказательной базы, позволяет с высокой долей вероятности избежать модификации уже собранных данных.

Мы приветствуем физическое присутствие специалистов заказчика на всех стадиях реагирования, сбора информации и расследования инцидента.

Наши отношения регулируются договором, соглашением о неразглашении информации и соглашением об уровне сервиса.

Мы привлекаем к реагированию и расследованию инцидентов компетентных сотрудников, которые дорожат своей репутацией в силу специфики их деятельности.

{ Кому в организации нужно расследование инцидентов? }

Как правило, расследование источников и причин совершенного киберпреступления в первую очередь интересно владельцам бизнеса. Ряд действий, нарушающих информационную безопасность организации и приводящих к утрате или порче информации, имеет заказной характер, и за этими действиями стоят конкретные заказчики.

Обычно собственникам интересен комплексный охват проблемы и ее полное, а не частичное решение и «разовые» меры по защите от инцидентов.

Услуги LETA IT-company и Group-IB позволяют заказчикам выявить исполнителей, найти «следы» совершенного преступления, прекратить активности злоумышленников в момент атаки и пресечь их на будущее, на основании собранных улик сделать выводы о заказчиках. Кроме того, услуги LETA IT-company и Group-IB позволяют дать достойный отпор информационным угрозам злоумышленников и пресечь дальнейшие противозаконные действия с их стороны в силу боязни полноценного уголовного преследования.

О компаниях

**LETA IT-company
Group-IB**

LETA IT-company – один из лидеров рынка информационной безопасности в России, первый оператор типизированных ИТ-услуг

LETA оказывает весь спектр услуг по информационной безопасности – от разработки стратегии ИБ до внедрения и сопровождения технических средств защиты информации. Портфель услуг LETA включает услуги и решения в области:

- управления ИБ (включая разработку стратегии ИБ, аудит ИБ, построение системы управления ИБ (СУИБ) в соответствии с ISO 27001, системы обеспечения непрерывности бизнес-процессов в соответствии с BS25999 и т.д.);
- соответствия требованиям Федерального закона № 152-ФЗ «О персональных данных», PCI DSS, СТО БР ИББС;
- обеспечения информационной безопасности (включая защиту от утечек информации (DLP), обеспечение безопасности при работе с Интернетом, защиту от вирусов и спама, атак и вторжений, контроль уязвимостей ПО и т.д.);
- защиты информационных ресурсов, собственником которых является государство (государственная тайна, служебная тайна), – в консорциуме с «ЛОТ».

Компания LETA занимает 3-е место среди крупнейших ИТ-компаний России в сфере защиты информации и является лидером российского рынка защиты от утечек данных и борьбы с инсайдерами. LETA IT-company входит в LETA Group – компанию № 1 по объему продаж на российском рынке продуктов и услуг в сфере информационной безопасности (по итогам рейтинга CNews Security 2009).

LETA IT-company обладает необходимыми лицензиями ФСБ России и ФСТЭК России на деятельность и осуществление работ в области защиты информации (включая осуществление работ, связанных с использованием сведений, составляющих государственную тайну).

LETA IT-company:

- является авторизованным партнером BSI (British Standards Institution);



- входит в ключевые объединения на рынках ИБ и ИТ:



- Association for Banking Information Security Standards (ABISS), объединяющее пользователей стандартов Центрального банка Российской Федерации по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС);



- межрегиональную общественную организацию «Ассоциация защиты информации» (АЗИ);



- Евро-Азиатскую ассоциацию производителей товаров и услуг в области безопасности (ЕВРААС);

- является партнером ведущих зарубежных и российских вендоров в сфере ИБ и ИТ, обладает партнерскими статусами высокого уровня у ключевых разработчиков;
- в рамках консорциумов с ключевыми игроками рынка ИБ и ИТ (Software AG & IDS Scheer, Digital Security, «ЛОТ», Cleverics) обеспечивает заказчикам дополнительные преимущества оказываемых услуг.



ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ И ОБЪЕКТОВ



Group-IB – первая и единственная в России компания, профессионально занимающаяся расследованием компьютерных преступлений и ИТ-инцидентов. Group-IB работает на российском рынке ИБ с 2003 года

Group-IB выполняет весь спектр работ, связанных с нарушением информационной безопасности частного или юридического лица, и обеспечивает:

- восстановление хронометража событий;
- выявление причин произошедшего инцидента;
- выявление лиц, причастных к инциденту;
- оказание информационной поддержки для предотвращения и профилактики инцидентов;
- юридическое сопровождение.

Group-IB проводит расследования:

- неправомерного доступа к компьютерной информации (в том числе атак и действий хакеров);
- создания, использования и распространения вредоносного программного обеспечения;
- корпоративных ИТ-инцидентов;
- мошенничества в сетях связи;
- покушений на права и свободы граждан, связанные с информационными технологиями.

Group-IB предоставляет заказчикам не только уникальный состав, но и уровень сервиса. Наряду с передовым комплексом профессионально оказываемых услуг Group-IB обеспечивает:

- молниеносное реагирование на инцидент (отражение DDoS-атаки, прибытие эксперта-криминалиста в пределах 1 часа);
- круглосуточную работу в режиме «24 x 7 x 365»;

- мировой охват деятельности и отлаженные партнерства с организациями, занимающимися расследованием компьютерных преступлений, в 43 странах мира (включая Россию – ФСБ, Управление «К», прокуратуру, суды);
- профессиональное, дорогостоящее оборудование и экспертный уровень в его применении;
- уникальную накопленную базу знаний;
- широкий спектр моделей оказания услуг (по составу и формату).

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

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 и благодаря этому могут применять лучшие технические средства по соблюдению конфиденциальности работ.

Group-IB является уникальным представителем в России группы следующих производителей программного и программно-аппаратного обеспечения информационной безопасности и компьютерной криминалистики:

- | | |
|-----------------|-------------------------|
| • GuardianEdge; | • DFLabs; |
| • Sourcefire; | • Forensic Technology; |
| • RSA; | • Paraben; |
| • Symantec; | • GetData; |
| • Belkasoft; | • COMPELSON Trade, Ltd. |

LETA IT-company и Group-IB входят в 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: DAMACK, HamsterSoft.
- **LETA Group Investment&Venture** — инвестиции в передовые ИТ-проекты.

www.letagroup.ru



LETA IT-company

ул. 8-я Текстильщиков, д. 11, стр. 2
г. Москва, Россия, 109129

+7 (495) 921 1410

+7 (495) 661 5538 (телефон оперативного дежурного)

<http://www.leta.ru>

<http://letablog.livejournal.com>

info@leta.ru

