

Расследование инцидентов ИБ

Уникальное предложение по раскрытию киберпреступлений и законодательному преследованию злоумышленников в сфере компьютерных технологий – первое и единственное в России!

Всегда ли Ваша служба информационной безопасности или информационных технологий:

- ? вовремя знает, что произошел инцидент информационной безопасности – например, несанкционированный доступ в системы, временная недоступность сервисов, вирус, атака на веб-сайты?
- ? готова остановить инцидент и минимизировать его последствия?
- ? умеет провести анализ инцидента и извлечь из него необходимые уроки?
- ? умеет правильно собрать электронные доказательства для обращения в правоохранительные органы?
- ? способна установить лиц, причастных к инциденту?
- ? способна оказать юридическое и техническое сопровождение уголовного дела и судебного процесса?

LETA IT-company и Group-IB впервые на российском рынке предлагают уникальный комплекс услуг по предотвращению, обнаружению, реагированию и расследованию инцидентов информационной безопасности (ИБ)

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**.

Статистика МВД РФ по количеству зарегистрированных преступлений в сфере компьютерной информации:

- 2007 г. – **7236**
- 2008 г. – **9010**
- 2009 г. (1-е полугодие) – **7595**

Предложение LETA IT-company и Group-IB обеспечивает:

- снижение корпоративных рисков, связанных с инцидентами информационной безопасности;
- расследование и правовое сопровождение любых внутренних и внешних инцидентов информационной безопасности;
- повышение осведомленности пользователей и администраторов ИС в вопросах обеспечения ИБ.

LETA IT-company и Group-IB предлагают 3 программы типизированных услуг по **предотвращению, обнаружению, реагированию и расследованию инцидентов ИБ**

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

Программа «Standard»

Стандартный набор сервисов, необходимый для реагирования и расследования инцидентов ИБ.

Реагирование на инциденты ИБ:

- оперативное дежурство и поддержка (круглосуточно: 7 дней в неделю, 365 дней в году):
 - 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).

Программа «Primary»

Расширенная программа, включающая все преимущества программы поддержки 1-го уровня «Standard», а дополнительно к ним:

Мониторинг защищенности и аудит ИБ:

- защита одного ресурса от распределенных атак на отказ в обслуживании;
- 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.

Программа «Premium»

Комплексный аутсорсинг службы реагирования на инциденты информационной безопасности – максимальная оперативность реагирования, постоянный контроль и эффективность принятых мер.

Включает все преимущества программ поддержки 1-го и 2-го уровня – «Standard» и «Primary», а дополнительно к ним:

Аутсорсинг команды реагирования:

- на территории Вашей организации или удаленно всегда находится минимум один специалист LETA IT-company и 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.

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 борьбе с киберпреступностью, а также получают лучшие рекомендации и технические средства по соблюдению конфиденциальности работ.

Все работы проводятся в соответствии с законодательством Российской Федерации. За основу LETA IT-company и Group-IB берут опыт международных организаций по расследованию ИТ-инцидентов, борьбе с компьютерной преступностью и кибертерроризмом.

Услуги по расследованию инцидентов ИБ оказываются компанией Group-IB в рамках стратегического партнерства с LETA IT-company.

Выгоды и преимущества

- **Уникальность.** LETA IT-company и Group-IB – первые и единственные в России, кто оказывает комплексные круглосуточные услуги по расследованию ИТ-инцидентов и компьютерных преступлений.
- **Финансовая эффективность.** За цену, эквивалентную зарплате одного опытного аудитора инцидентов информационной безопасности, Вы получаете команду с многолетним опытом и необходимым оборудованием, готовую среагировать на Ваш вызов в любое время, 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 информационной безопасности.
- **Соответствие 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. 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 3-й стороны – в соответствии с рекомендациями международных стандартов.
- **Широкая география деятельности.** Расследования возможны в 43 странах мира.
- **Экономия.** Вам не нужно покупать дорогостоящее оборудование для проведения компьютерной экспертизы.
- **Повышение культуры безопасности в компании.** Проведение расследований наглядно демонстрирует торжество правосудия и неотвратимость наказания за правонарушение. Осознание ответственности и последствий совершения компьютерного преступления – лучшее средство обеспечения информационной безопасности организации в будущем.
- **Эффективное использование человеческих ресурсов.** Услуга LETA IT-company и Group-IB позволяет не отрывать сотрудников от повседневной работы и не проводить дорогостоящее обучение расследованиям компьютерных инцидентов.
- **Постоянный контроль рисков ИБ.** LETA IT-company и Group-IB обеспечивают регулярное проведение оценки рисков ИБ.
- **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.

Group-IB («Группа информационной безопасности», www.group-ib.ru) – первая в России компания, профессионально занимающаяся расследованием компьютерных преступлений и ИТ-инцидентов с 2003 года.

LETA IT-company – один из лидеров рынка информационной безопасности в России, первый оператор типизированных ИТ-услуг. Компания LETA оказывает весь спектр услуг по информационной безопасности – от разработки стратегии ИБ до внедрения и сопровождения технических средств защиты информации.



LETA IT-company

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

Тел./факс: +7 (495) 921 1410

E-mail: info@leta.ru

<http://www.leta.ru>

<http://letablog.livejournal.com>