

КОМПЛЕКСНОЕ РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА





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, публичной 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 всего документа или его части допускается лишь с письменного разрешения Group-IB. При цитировании документа ссылка на источник заимствования обязательна.



СОДЕРЖАНИЕ

СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ	3
МОШЕННИЧЕСТВО В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА	5
КОМПЛЕКСНОЕ РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА	9
Шаг 1. Реагирование	10
Шаг 2. Исследование носителей информации	12
Шаг 3. Расследование	15
Шаг 4. Юридическое сопровождение	17
Шаг 5. Аудит информационной безопасности	19
ЗНАЧИМОСТЬ И ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РАССЛЕДОВАНИЯ	23
О КОМПАНИИ GROUP-IB	22
О КОМПАНИИ LETA GROUP	24





СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Стремительное развитие информационных технологий серьезно изменило подходы к организации современного бизнеса. Несомненные преимущества, которые несут в себе ИТ, позволили вести бизнес более эффективно, автоматизируя функциональные процессы. Технологии стерли границы и расстояния, привели к глобализации операций. Например, сегодня можно хранить корпоративные данные на сервере в Сингапуре, осуществлять платежи в Лондоне или оказывать услуги американским партнерам, находясь в Москве.

За последнее время системы дистанционного банковского обслуживания (ДБО) стали неотъемлемой частью взаимодействия коммерческих организаций с банками. Все чаще финансовые операции совершаются с помощью интернета, а возможность удаленного доступа к банковским услугам в режиме реального времени играет важную роль в формировании современного бизнеса. Удобство применения таких систем трудно недооценить: они позволяют снизить издержки и повысить оперативность проведения финансовых операций.

Дистанционное банковское обслуживание — это комплекс сервисов удаленного доступа клиентов к банковским услугам. При этом клиент удаленно (без визита в банк) передает необходимые распоряжения, используя в основном информационные технологии.

Существует большое количество терминов, которые используются как синонимы для описания услуг дистанционного банковского обслуживания через интернет: клиент-банк, банк-клиент, интернет-банкинг, электронный банкинг и пр. В том числе встречаются и англоязычные варианты обозначений: online banking, remote banking, e-banking, home banking, internet banking и т.д.

Однако, несмотря на такое количество терминов, связанных с наиболее распространенным видом ДБО, системы электронного банкинга сводятся к двум основным типам систем:

- Клиент-банк.
- Интернет-клиент.

Первая система, как правило, направлена на обслуживание банком юридических лиц, тогда как вторая — на обслуживание лиц физических. Обе они объединены тем, что доступ к системе осуществляется через персональный компьютер и для соединения с банком используется сеть интернет. Принципиальное отличие сводится к тому, что для системы «Клиент-банк» нужно устанавливать на компьютере специальную программу, тогда как для системы «Интернет-клиент» достаточно обычного браузера.

СХЕМА ДБО



В итоге дистанционное банковское обслуживание является удобной формой взаимодействия банка и клиента, которое несет определенные выгоды обеим сторонам. Удобство, доступность, оперативность и разнообразие — главные преимущества, которые сделали дистанционное банковское обслуживание неотъемлемой частью взаимодействия коммерческих организаций с банками.



МОШЕННИЧЕСТВО В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА

К сожалению, помимо очевидных преимуществ, активное применение информационных технологий добавило новые риски, с которыми многие до этого не сталкивались и даже не знали об их существовании. С приходом высоких технологий в мир бизнеса одной из важнейших угроз является вмешательство киберпреступников в работу финансовых учреждений.

Экспертам в области расследования компьютерных преступлений приходится ежедневно сталкиваться с различными инцидентами, которые, так или иначе, затрагивают интересы финансовых организаций: DDoS-атаки (распределенные атаки на отказ в обслуживании), мошенничество в системах дистанционного банковского обслуживания, взлом серверов и хищение конфиденциальной информации, очернение репутации путем размещения в интернете клеветы и оскорблений. Каждый из этих инцидентов негативно отразился на деятельности пострадавших компаний. Однако из всего вышеперечисленного наибольший финансовый ущерб наносят мошенничества в системах интернет-банкинга.

Методы мошенников

Наиболее распространенный сценарий совершения мошенничеств в системах интернет-банкинга состоит из трех основных этапов: получение информации для осуществления неправомерного доступа в систему «Клиент-банк», проведение мошеннической операции и обналичивание денег.

1. Получение информации для доступа в систему дистанционного банковского обслуживания

Для хищения авторизационных данных пользователя системы дистанционного банковского обслуживания: логина, пароля и ключей электронной подписи — злоумышленники используют специальное вредоносное программное обеспечение. Чаще всего это модификации хорошо известных банковских троянов Zeus, SpyEye, Carberp с дополнительным функционалом.

Схема работы таких вирусов следующая. Сотрудник компании посещает зараженный веб-сайт, с которого на его компьютер, используя ту или иную уязвимость, загружается вредоносная программа, которая обходит антивирусную защиту и другие виды защит. Попадая на компьютер, такая программа определяет, с какими приложениями работает пользователь. При обнаружении следов работы с системами дистанционного банковского обслуживания или системами электронных денег на компьютер дозагружаются вредоносные модули, предназначенные для хищения авторизационных данных пользователя. Все эти данные вместе с сопутствующей информацией, например, о количестве денег на счетах, попадают в руки злоумышленникам. Современные банковские трояны имеют широкий функционал и способны работать



15 000 000 \$

**самый крупный ущерб
организации, который
фиксировали
специалисты
Group-IB**

одновременно с несколькими системами дистанционного банковского обслуживания, обеспечивая киберпреступникам возможность удаленного доступа и сокрытия следов преступлений.

2. Проведение мошеннической операции

При получении данных от трояна, мошенники проверяют полученные сведения и определяют возможности для совершения преступления. Определяющую роль на данном этапе играют средства защиты, применяемые банком и его клиентом.

ТИПОВАЯ СХЕМА МОШЕННИЧЕСКОЙ ОПЕРАЦИИ*

***СУЩЕСТВУЮТ И ДРУГИЕ МОШЕННИЧЕСКИЕ СХЕМЫ**



Для отправки подложного платежного поручения злоумышленники могут использовать различные возможности вредоносных программ. Например, возможна отправка платежного поручения непосредственно с компьютера клиента банка с использованием средств удаленного управления. Или автоматическое формирование мошеннического платежного поручения вирусом и подмена вредоносной программой реквизитов легитимного платежного поручения за мгновение до его подписания и передачи в банк.

Как только платежное поручение отправлено, главная задача злоумышленников — ограничить доступ легитимного пользователя к системе «Клиент-банк». Для этой цели могут использоваться различные методы: смена пароля от системы интернет-банкинга, вывод из строя компьютера пользователя, DDoS-атака на сервер банка. Чаще всего повреждают файловую систему жесткого диска пользователя или удаляют один из компонентов операционной системы. В то время, пока все силы клиента банка брошены на восстановление работоспособности компьютера, деньги покидают его счет и попадают в руки преступников.

3. Обналичивание похищенных денежных средств

Этот этап чаще всего выполняют специализированные группы лиц, которые обладают тесными связями с организованными преступными группировками. Схема обналичивания начинается еще во время подготовки к хищению денег, так как она зависит от суммы денежных средств, которую предстоит вывести. В случае небольших сумм (до 2 млн. рублей), чаще всего, используются пластиковые карты физических лиц, причем предпочтительны карты тех банков, в которых имеются большие лимиты по выдаче наличных средств в банкоматах. В случае крупных сумм используется цепочка счетов подставных компаний и физических лиц, в ходе переводов сумма дробится для облегчения снятия наличных денег через банкомат.

ТИПОВАЯ СХЕМА ОБНАЛИЧИВАНИЯ ПОХИЩЕННЫХ СРЕДСТВ*

***СУЩЕСТВУЮТ И ДРУГИЕ МОШЕННИЧЕСКИЕ СХЕМЫ**



По данным МВД России, только в Москве каждый месяц происходит больше десятка успешных мошеннических операций с использованием систем дистанционного банковского обслуживания. Средний ущерб по каждому инциденту составляет 3 млн. рублей. Помимо этого, ежедневно сотрудниками служб безопасности банков пресекаются попытки мошенничества на суммы в сотни миллионов рублей. Широкое распространение мошенничества в системах «Клиент-банк» связано с возможностью получить многомиллионные сверхприбыли.



КОМПЛЕКСНОЕ РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА

Мошенничество в системах дистанционного банковского обслуживания требует оперативной и компетентной реакции. Только быстрые и слаженные действия специалистов службы безопасности банка, пострадавшего клиента, независимых криминалистов и сотрудников правоохранительных органов позволяют предотвратить хищение, вернуть денежные средства и поймать злоумышленников. Если факт инцидента обнаружен в течение 12 часов с момента его совершения, то вероятность возврата денежных средств в течение нескольких рабочих дней близка к 90%. Любые промедления чреваты серьезным затруднением процесса расследования и даже безвозвратной потерей денег.

Комплексное расследование мошенничества в системах интернет-банкинга состоит из пяти последовательных шагов:

1. реагирование на инцидент и сбор доказательной базы;
2. криминалистическое исследование «цифровых» следов инцидента;
3. непосредственное расследование инцидента и выявление лиц, причастных к мошенничеству;
4. юридическое сопровождение и представление интересов в рамках расследования уголовного дела и судебного разбирательства;
5. постинцидентный консалтинг и улучшение степени защищенности систем дистанционного банковского обслуживания.

Указанный комплекс мер позволяет разобраться в произошедшем инциденте, идентифицировать злоумышленников и привлечь их к ответственности, компенсировать понесенный ущерб, а также избежать повторных хищений денежных средств с банковского счета.

Успешные примеры по пресечению и расследованию случаев мошенничества показывают, что в настоящее время компьютерные преступники в отличие от прошлых лет не всегда выходят «сухими из воды». Постоянное развитие услуг и методов реагирования на компьютерные инциденты, тесное сотрудничество с российскими и иностранными правоохранительными органами, а также компетентное представление интересов пострадавших компаний в судах позволяет специалистам Group-IB результативно отвечать на преступные действия мошенников.

Шаг 1. Реагирование на мошенничество в системах интернет-банкинга

Постоянное увеличение числа случаев данного вида преступлений и масштабы наносимого финансового ущерба ставят перед компаниями вопрос о своевременном реагировании на мошенничества в системах дистанционного банковского обслуживания. Несмотря на сложные схемы преступлений в системах интернет-банкинга, группы злоумышленников оставляют следы незаконной деятельности, по которым они могут быть идентифицированы и привлечены к ответственности.

Специалисты Group-IB предлагают полный спектр услуг по реагированию на инциденты информационной безопасности в системах дистанционного банковского обслуживания, который заключается в сборе, обеспечении сохранности и оформлении доказательной информации для последующего криминалистического исследования и передачи в правоохранительные органы.

В случае обнаружения признаков мошенничества достаточно обратиться в Group-IB и описать оперативному дежурному суть проблемы. В течение кратчайшего времени Группа оперативного реагирования прибудет на место инцидента и проведет сбор необходимых цифровых доказательств, независимое криминалистическое исследование которых поможет определить обстоятельства произошедшего инцидента. Помимо этого, специалисты Group-IB подготовят необходимый пакет документов для передачи в правоохранительные органы, а также проконсультируют представителей пострадавшей стороны по вопросам минимизации ущерба, связанного с наступившим инцидентом.

СХЕМА РЕАГИРОВАНИЯ



При выезде на место инцидента наши специалисты Лаборатории компьютерной криминалистики и восстановления данных проводят:

- поиск, извлечение и копирование сведений, имеющих отношение к инциденту информационной безопасности, с помощью специализированного программного и программно-аппаратного обеспечения;
- юридически грамотное оформление процедуры изъятия и копирования информации;
- опечатывание и передача носителей информации на ответственное хранение.

Обнаружение, сбор и сохранение необходимых данных об инциденте, а также юридически грамотное оформление соответствующих документов, является одной из главных задач после выявления факта мошенничества, которая зачастую не под силу штатным ИТ-специалистам. Ошибки, допущенные на этом этапе, могут в последующем уничтожить «цифровые» следы преступления или привести к признанию собранных доказательств недопустимыми.

Криминалисты Group-IB обладают соответствующими знаниями, большим опытом работы, а также специализированным оборудованием и программным обеспечением — всем тем, что необходимо для минимизации рисков потери доказательственной информации или возможности последующего ее отвода в суде как собранной с нарушением процессуального законодательства.

Эксперты Group-IB выполняют работы, связанные с реагированием на мошенничество в системах дистанционного банковского обслуживания:

- немедленная консультация сертифицированных специалистов в режиме 24x7;
- оперативная разработка и помощь в реализации плана реагирования на инцидент;
- юридическое сопровождение всех производимых работ с учетом сохранения доказательной базы и дальнейшего сопровождения инцидента;
- оперативное устранение критичных уязвимостей;
- разработка рекомендаций по улучшению мер защиты информации;
- разработка плана и набора рекомендаций по расследованию инцидента;
- предоставление информации по первоначальным этапам расследования и рекомендаций по оперативному восстановлению бизнес-процессов;
- предоставление полного отчета об инциденте, включающего информацию о проведенных Group-IB мероприятиях.

В результате процесса реагирования специалисты Group-IB проводят сбор и сохранение доказательной базы, а также предоставляют юридическую консультацию по вопросам привлечения к ответственности лиц, причастных к инциденту, и техническую консультацию с целью повышения безопасности информационной системы и предотвращения повторных инцидентов.

Следующий шаг: передача копий носителей с собранной доказательной информацией в Лабораторию компьютерной криминалистики и восстановления данных Group-IB для дальнейшего криминалистического исследования и выяснения методов совершения мошенничества.

Шаг 2. Исследование носителей информации с целью поиска и оформления доказательств

Проведение криминалистического исследования является важной частью процесса реагирования и расследования мошенничества в системах интернет-банкинга. 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 правильных методик и инструментов.

Лаборатория компьютерной криминалистики и восстановления данных Group-IB является специализированным подразделением, занимающимся проведением экспертных исследований в области информационных технологий и компьютерной криминалистики, а также восстановлением данных с различных носителей информации. Независимые исследования и судебные экспертизы, проводимые специалистами лаборатории, служат важнейшими источниками информации при разборе правонарушений, раскрывают методы и цели совершения противоправных действий, а также указывают на причастных лиц. В рамках коммерческих и судебных криминалистических исследований компьютерной информации решаются следующие вопросы:

- о наличии признаков несанкционированного доступа к информационной системе и обрабатываемой в ней информации;
- о наличии информации в явном и неявном (скрытом, удаленном или зашифрованном) видах по заданным критериям (ключевым словам);
- о наличии заданного программного обеспечения в установленной форме либо в форме дистрибутива, а также об их конфигурации;
- о хронологии событий в информационной системе;
- о неизменности (целостности) компьютерной информации после изъятия или исследования;
- о наличии вредоносных программ, а также о функциональных возможностях таких программ в случае их обнаружения.

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.

По итогам проведения криминалистических исследований предоставляются:

- хронология событий инцидента;
- причины возникновения инцидента, в частности степень участия в этом сотрудников потерпевшей стороны;

- комплексный список рекомендаций по полному восстановлению инфраструктуры информационной системы;
- необходимые сведения для дальнейшего расследования инцидента информационной безопасности (IP-адреса, доменные имена, псевдонимы злоумышленников в сети, адреса электронной почты, идентификационные данные программ мгновенного обмена сообщениями и т. п.).

В процессе криминалистического исследования специалисты Group-IB проводят анализ «цифровых следов» злоумышленников и устанавливают, каким образом было совершено мошенничество. Параллельно криминалисты проводят восстановление удаленных и поврежденных преступниками данных. Результатом работы экспертов Group-IB являются отчеты, оформленные в соответствии с действующим законодательством, которые позволяют использовать их в дальнейших расследованиях и судебных разбирательствах.

Следующий шаг: передача результатов криминалистического исследования в Отдел расследований Group-IB для выявления лиц, причастных к совершению мошенничества.



A young man with glasses, wearing a red long-sleeved shirt and grey trousers, is kneeling in a server room. He is focused on a laptop that is resting on a server rack. The room is filled with rows of server racks, and many cables are visible, some bundled together. The floor is a light-colored, perforated metal grating. The background shows more server racks and the perforated metal doors of the racks.

Расследование инцидентов ИБ — уникальная для России услуга, предоставляемая Group-IB. Она обеспечивает компаниям, столкнувшимся с хищением денежных средств с банковского счета, неотвратимость ответственности злоумышленников за совершенные правонарушения и высокую вероятность возмещения нанесенного ущерба.

Шаг 3. Расследование мошенничества в системах интернет-банкинга

Комплексное расследование случаев мошенничества в системах дистанционного банковского обслуживания предполагает выявление исполнителя, его фактическое местонахождение, грамотный сбор улик и доказательств преступления, а также предоставление материалов в правоохранительные органы для юридического преследования злоумышленника и привлечения его к ответственности.

Для выполнения подобных задач необходимы специальный штат и высокая квалификация специалистов — владение методиками и процедурами сбора и представления доказательств, их подачи в компетентные инстанции, знание законодательных норм и тонкостей данного вида преступлений. Поэтому специалисты Group-IB предоставляют комплекс услуг по расследованию мошенничества в системах интернет-банкинга и иных компьютерных преступлений.

Расследования мошенничества в системах интернет-банкинга состоят из следующих этапов:

- поиск следов причастности внутренних сотрудников (по результатам криминалистического исследования);
- выявление панелей управления вредоносным программным обеспечением и поиск связей с другими инцидентами информационной безопасности;
- выявление лиц, оказывающих дополнительные услуги злоумышленнику;
- получение детальных сведений о структуре панели управления вредоносным программным обеспечением и получение доказательств о ее использовании в конкретном мошенничестве в интернет-банкинге;
- установление лица, управляющего бот-сетью, и его фактического местонахождения;
- оформление всех полученных данных в виде комплекта документов для последующей передачи в правоохранительные и судебные органы.

Во время проведения расследования осуществляется целый ряд исследований вредоносного программного обеспечения, управляющих серверов и иных данных. Для получения подобной информации Group-IB активно использует собственную сеть ловушек HoneyNet, состоящую из 30 тысяч сенсоров, и тесные контакты с экспертными подразделениями в 48 странах мира.

Результатом работы экспертов Group-IB является комплексный отчет, оформленный в соответствии с действующим законодательством, который позволяет использовать полученные сведения в расследованиях, проводимых правоохранительными органами, и дальнейших судебных разбирательствах.

Следующий шаг: передача результатов проведенного расследования специалистами Юридического отдела Group-IB в правоохранительные и судебные органы для привлечения злоумышленников к ответственности и компенсации понесенного ущерба.

Только грамотное использование сотрудниками юридического отдела Group-IB правовых норм в вопросах, связанных с информационной безопасностью, обеспечивает пострадавшим компаниям правовую защищенность. При расследовании случаев мошенничества в системах интернет-банкинга юридическое сопровождение дел в правоохранительных органах и судах позволяет привлечь злоумышленников к ответственности, а также возместить ущерб и финансовые средства, потраченные на сбор потерпевшей стороной доказательств.



Шаг 4. Юридическое сопровождение расследований мошенничества в системах интернет-банкинга

Комплексное расследование случаев мошенничества в системах дистанционного банковского обслуживания невозможно без передачи результатов проведенных работ в правоохранительные органы. Только в тесном сотрудничестве с ними можно добиться, чтобы злоумышленники понесли заслуженное наказание.

Однако не всегда пострадавшие от рук мошенников знают, куда нужно направиться по вопросам, связанным с защитой их прав в сфере информационных технологий. Еще реже они понимают, каким образом доказать, что их права нарушены, и как добиться справедливости.

Часто те, кто столкнулся с инцидентами информационной безопасности, обращаются за помощью в юридические компании, большинство из которых не обладают достаточными знаниями в сфере информационных технологий. В итоге во время представления интересов клиента в правоохранительных и судебных органах используются не все возможные правовые тонкости расследования компьютерных преступлений.

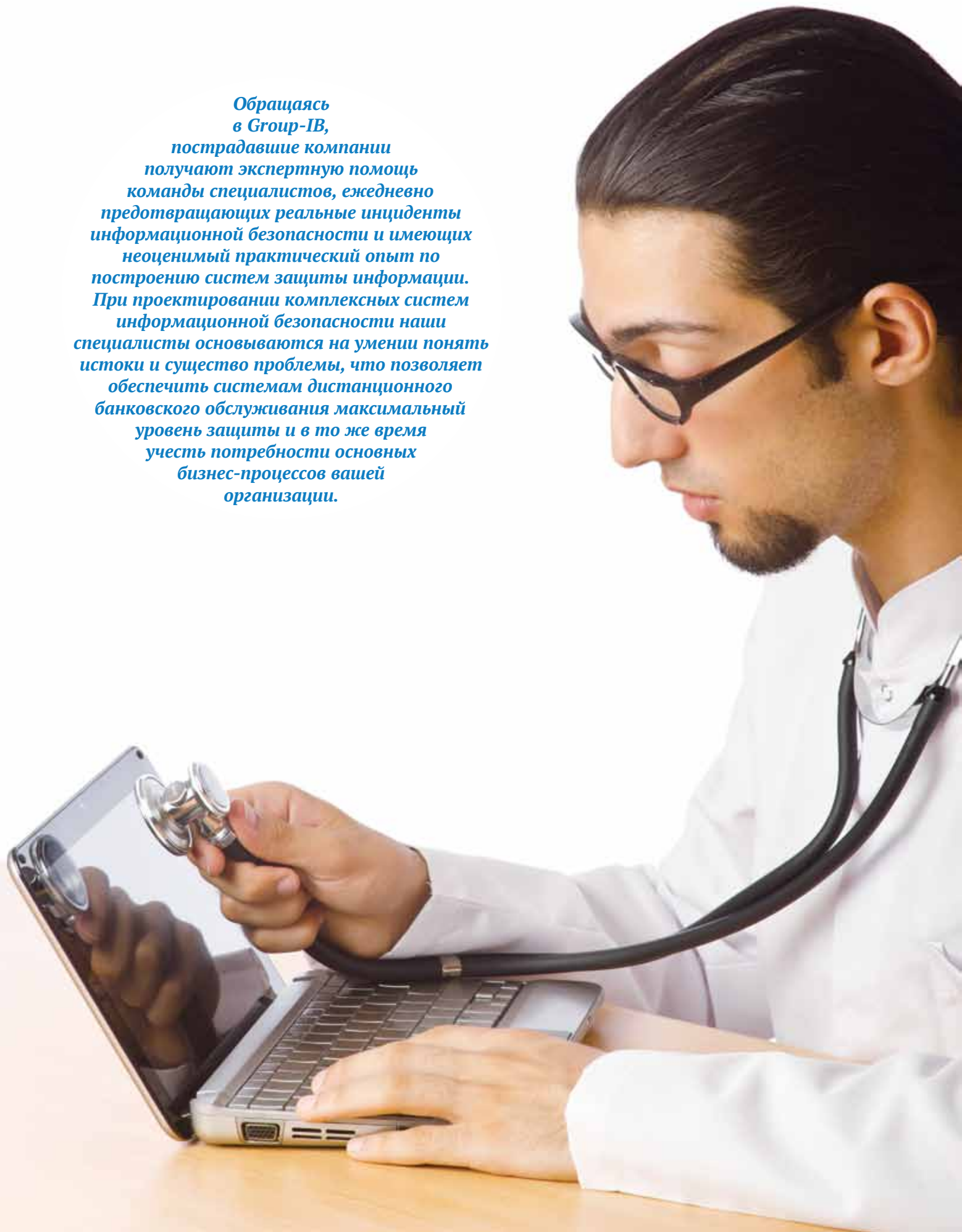
Специалисты юридического отдела Group-IB оказывают полный спектр услуг по защите интересов пострадавшей стороны в судах, правоохранительных органах и иных государственных структурах по вопросам расследования хищений денежных средств с банковских счетов и иных компьютерных правонарушений:

- оформление информации (доказательств) в качестве юридически значимой доказательной базы;
- консультации по уровню компетенции правоохранительных органов, в которые необходимо передать заявление и комплект документов;
- помощь в оформлении документов и последующей их передаче в компетентные правоохранительные, надзорные и регулирующие органы, а также суды;
- сопровождение проверки и расследования с момента подачи заявления до момента возбуждения уголовного дела или передачи дела с обвинительным заключением в суд;
- представление интересов в рамках уголовного судопроизводства.

Однако наказание преступников и восстановление справедливости не всегда является наглядным примером для остальных компьютерных злоумышленников. Важно, обеспечить неповторение самого факта мошенничества.

Поэтому **следующий шаг**: проведение специалистами Отдела аудита и консалтинга Group-IB аналитического исследования степени защищенности используемых системы дистанционного банковского обслуживания с последующим построением систем управления инцидентами информационной безопасности и непрерывностью бизнеса.

*Обращаясь
в Group-IB,
пострадавшие компании
получают экспертную помощь
команды специалистов, ежедневно
предотвращающих реальные инциденты
информационной безопасности и имеющих
неоценимый практический опыт по
построению систем защиты информации.
При проектировании комплексных систем
информационной безопасности наши
специалисты основываются на умении понять
источники и существо проблемы, что позволяет
обеспечить системам дистанционного
банковского обслуживания максимальный
уровень защиты и в то же время
учесть потребности основных
бизнес-процессов вашей
организации.*



Шаг 5. Аудит информационной безопасности при расследовании случаев мошенничества в системах интернет-банкинга

Консалтинг в области пресечения хищений в системах интернет-банкинга подразделяется на два основных вида: превентивный и постинцидентный. Первый вид, основанный на проектировании и экспертном анализе возможных инцидентов информационной безопасности, помогает выстраивать систему защиты, нацеленную на предотвращение вероятных мошенничеств в системах дистанционного банковского обслуживания. Второй вид базируется на непосредственном анализе уже произошедших хищений, которые отражают существующие пробелы в системе защиты организации. Полученные данные позволяют обезопасить информационную инфраструктуру не только от возможных угроз, но и от повторения произошедших инцидентов.

В рамках предотвращения мошенничеств в системах интернет-банкинга специалисты Group-IB проводят оценку текущего уровня защищенности от внутренних и внешних угроз, а также формулируют и реализуют меры по обеспечению безопасности информации в соответствии с бизнес-процессами вашей организации. Эксперты Group-IB выполняют следующий спектр работ в области предупреждающего аудита и консалтинга по информационной безопасности:

- комплексный аудит информационной безопасности;
- аудит системы управления информационной безопасностью;
- аудит соответствия стандартам по информационной безопасности;
- аналитическое исследование защищенности систем ДБО от мошенничества;
- аудит защищенности рабочего места бухгалтера.
- анализ уязвимостей и тесты на проникновение;
- построение систем управления информационной безопасностью и непрерывностью бизнеса.

В рамках реагирования и расследования мошенничества в системах интернет-банкинга специалисты Group-IB проводят оценку существующих систем информационной безопасности, а также формулируют и реализуют меры по недопущению повторений произошедших инцидентов. Эксперты Group-IB выполняют следующий спектр работ в области постинцидентного аудита и консалтинга по информационной безопасности:

- комплексный аудит информационной безопасности;
- создание комплексного списка рекомендаций по полному восстановлению инфраструктуры информационной системы;
- разработка рекомендаций по улучшению мер защиты информации;
- 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.

ЗНАЧИМОСТЬ И ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РАССЛЕДОВАНИЯ

Реагирование на хищение денежных средств с банковских счетов, его расследование и проведение криминалистического исследования является необходимым условием для выявления истинных причин случившегося и помощи в минимизации ущерба.

В результате оказания нашими экспертами комплексных услуг по расследованию мошенничеств в системах дистанционного банковского обслуживания вы получаете:

1. Доказательную информацию, собранную и сохраненную в соответствии с требованиями действующего законодательства. Только участие высококвалифицированных специалистов, обладающих соответствующими компетенциями, позволяет минимизировать риск уничтожения важных для дальнейшего расследования доказательств и отвода их судом и правоохранительными органами вследствие некорректного сбора.
2. Юридическую и техническую консультацию, предоставляемые еще на стадии реагирования на инцидент. В каждом отдельном случае наши специалисты разработают оперативный план мер по остановке инцидента и воспрепятствованию его дальнейшему развитию, проконсультируют по вопросам правового преследования злоумышленников, помогут составить и оформить пакет документов и заявление для подачи в правоохранительные органы.
3. Уверенность в причастности или не причастности сотрудников вашей компании к случившемуся инциденту. В результатах по итогам расследования инцидента в обязательном порядке указывается хронология и методы совершения мошенничества, а также предоставляются полученные в ходе исследования идентификационные данные злоумышленников. В случае внутреннего инцидента получить такую информацию особенно важно, так как она позволяет выявить нечестных сотрудников, действующих во вред вашей компании.
4. Заключение экспертов, принимаемое правоохранительными органами и судебными инстанциями в качестве допустимого доказательства при проведении гражданского, административного и уголовного производства. Результаты независимых криминалистических исследований, проводимых сертифицированными специалистами Group-IB, высоко ценятся как в России, так и за ее пределами и активно используются как правоохранительными органами, так и судами.
5. Возможность правового преследования злоумышленников и компенсации ущерба. Сочетание методов оперативного реагирования и компьютерной криминалистики, а также знание особенностей действующего законодательства позволяют не только идентифицировать злоумышленников, но и привлечь их к ответственности с последующей компенсацией ущерба и издержек, вызванных инцидентом.

6. Рекомендации по повышению защищенности инфраструктуры вашей компании. По завершению реагирования на инцидент специалисты Group-IB предоставляют перечень выявленных уязвимостей в системе информационной безопасности, которые являлись причиной инцидента, а также комплексный список рекомендаций по их устранению и полному восстановлению ИТ-инфраструктуры.

Обратившись в Group-IB, вы получаете команду компетентных специалистов в области компьютерной криминалистики, информационной безопасности и юриспруденции, которые выполняют все необходимые работы с момента получения сообщения об инциденте до передачи материалов в правоохранительные органы с возможностью дальнейшего представления Ваших интересов во время расследования и судебного разбирательства. Успех такого подхода нашел свое отражение в многочисленных благодарственных письмах от наших клиентов, с которыми мы продолжаем эффективно сотрудничать и по сей день.

О КОМПАНИИ GROUP-IB



Основанная в 2003 году, компания Group-IB является первой в России и в странах СНГ компанией, профессионально и комплексно занимающейся расследованием обстоятельств компьютерных преступлений, нарушений информационной безопасности и компьютерной криминалистикой. Входит в состав Leta Group.

Основные услуги Group-IB:

- расследование любых инцидентов информационной безопасности;
- мониторинг и реагирование на инциденты в режиме 24/7;
- компьютерная криминалистика;
- расследование мошенничеств в системах интернет-банкинга;
- расследование и защита от DDoS-атак;
- защита брендов от интернет-угроз;
- юридическое и правовое сопровождение;
- аудит и консалтинг по обеспечению информационной безопасности;
- восстановление данных.

Group-IB — единственная компания, которая предлагает услуги обеспечения информационной безопасности в режиме «24x 7x365».

Эксперты компании разрабатывает методики предотвращения и расследования современных компьютерных преступлений, например, таких как DDoS-атаки, мошенничество в ДБО, взлом и кража конфиденциальной информации.

В составе Group-IB работает Лаборатория компьютерной криминалистики, оказывающая услуги независимой компьютерно-технической экспертизы, в том числе правоохранительным органам Российской Федерации.

Компетенции

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);
- круглосуточное дежурство в режиме «24 x 7 x 365»;
- тесное сотрудничество с правоохранительными органами Российской Федерации;
- мировой охват деятельности и отлаженное партнерство с организациями, занимающимися расследованием компьютерных преступлений, в 48 странах мира;
- профессиональное дорогостоящее оборудование и экспертный уровень его применения;
- 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.

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.

Наши партнеры

Group-IB является ведущим партнером следующей группы производителей уникального программного и программно-аппаратного обеспечения информационной безопасности и компьютерной криминалистики:

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



О КОМПАНИИ 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 промышленные инновации в промышленности. Компании Дивизиона: ASK Labs, АСКОМ-строй.

LETA Group Software Development — создание корпоративного и «домашнего» программного обеспечения. Компании Дивизиона: ДАМАСК, HamsterSoft.

LETA Group Investment & Venture — инвестиции в передовые ИТ-проекты.



Group-IB
Россия, г. Москва,
Мажоров переулок, д.14, стр.2.
Тел.: +7(495) 661-55-38
e-mail: info@group-ib.ru
www.group-ib.ru, www.letagroup.ru