ИНСТРУКЦИЯ

по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания

Автор: М. А. Суханов
Рецензенты: С. А. Грудинов и А. В. Лукацкий

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время наблюдается рост числа инцидентов в системах дистанционного банковского обслуживания, приводящих к большим финансовым потерям юридических и физических лиц и наносящих ущерб репутации банков.

К сожалению, в рамках проводимых нашей компанией расследований были зафиксированы множественные случаи некорректного реагирования на инциденты, в ходе которых системными администраторами, сотрудниками подразделений информационной безопасности организаций или иными уполномоченными лицами были уничтожены криминалистически значимые данные, позволяющие привлечь к уголовной ответственности злоумышленников, или была существенно снижена юридическая значимость данных, собранных в ходе внутреннего расследования инцидента.

Нередко в организациях, столкнувшихся с инцидентами в системах дистанционного банковского обслуживания в первый раз, системные администраторы и сотрудники подразделений информационной безопасности не знают, как реагировать на возникший инцидент, в каких случаях нужно обращаться в правоохранительные органы и как обеспечить оперативный сбор данных, необходимых для проведения расследования. Недостаток этих сведений приводит к позднему реагированию на инцидент, в результате которого платежные поручения, переданные злоумышленником, исполняются, а информационные следы действий злоумышленника удаляются.

Разработанная нами инструкция предназначена, в первую очередь, для повышения осведомленности заинтересованных лиц в вопросах реагирования на инциденты в системах дистанционного банковского обслуживания. Кроме того, наша инструкция может выступать основой для разработки внутренних нормативных документов организаций, регламентирующих процесс реагирования на инциденты.

В инструкции сознательно не рассматриваются вопросы организации системы управления инцидентами информационной безопасности, а также вопросы создания специализированных групп реагирования на инциденты информационной безопасности (CERT/CSIRT). Причиной этому является громоздкость данных вопросов, диктующая необходимость их рассмотрения в отдельных документах.

М. А. Суханов

ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая инструкция предназначена для использования работниками подразделений (служб) информационной безопасности организаций, техническими специалистами, оказывающими услуги по реагированию на инциденты безопасности, и иными лицами (например, системными администраторами), ответственными за безопасное функционирование элементов вычислительных сетей организаций, при реагировании на инциденты информационной безопасности, связанные с мошенничеством в системах дистанционного банковского обслуживания (интернет-банкинга).

Положения инструкции могут использоваться для разработки внутренних нормативных документов, определяющих способы реагирования на некоторые виды инцидентов информационной безопасности.

НОРМАТИВНО-ТЕХНИЧЕСКИЕ ДОКУМЕНТЫ

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
- Документ RFC 2828 «Internet Security Glossary».
- Документ RFC 3227 «Guidelines for Evidence Collection and Archiving».
- Документ «Good Practice Guide for Computer-Based Electronic Evidence» Ассоциации старших офицеров полиции (ACPO).

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И АББРЕВИАТУРЫ

ИНЦИДЕНТ, ХАРАКТЕР ИНЦИДЕНТА

Инцидент (или инцидент информационной безопасности) — системное событие, в рамках которого произошло нарушение политики безопасности (в соответствии с определением из документа RFC 2828).

Внешний инцидент (или инцидент, имеющий внешний характер) — инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом.

Внутренний инцидент (или инцидент, имеющий внутренний характер) — инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или другими способами).

Инцидент в системе дистанционного банковского обслуживания (или инцидент, связанный с мошенничеством или покушением на совершение мошенничества в системе дистанционного банковского обслуживания) — внешний или внутренний инцидент, в результате которого были созданы, подписаны с помощью электронной подписи и переданы в банк платежные поручения без санкции со стороны уполномоченных на совершение указанных действий лиц.

РЕАГИРОВАНИЕ И РАССЛЕДОВАНИЕ

Реагирование на инцидент — совокупность действий, направленных на выявление компьютерной информации, имеющей отношение к инциденту, и сохранение ее целостности и юридической значимости, а также на сбор иных сведений, имеющих отношение к инциденту.

Расследование инцидента — исследование компьютерной информации и иных сведений с целью установления обстоятельств инцидента (характера, временной шкалы и других фактов) и выявления причастных лиц.

ДРУГИЕ ПОНЯТИЯ

Компьютерная информация — информация на машинном носителе, в электронно-вычислительной машине, системе электронно-вычислительных машин или их сети.

Криминалистически значимые данные — компьютерная информация, используемая для обоснования выводов криминалистических исследований и позволяющая решить поставленные перед криминалистическим исследованием задачи.

Энергонезависимый носитель информации — машинный носитель информации, способный хранить записанную в него информацию в течение длительного времени без необходимости подключения к источнику питания (примеры: компакт-диск, накопитель на жестких магнитных дисках, флеш-накопитель, дискета).

Энергонезависимые данные — информация, содержащаяся на энергонезависимом носителе информации.

Энергозависимый носитель информации — машинный носитель информации, не способный после отключения от источника питания в течение длительного времени хранить записанную в него информацию (пример: оперативное запоминающее устройство).

Энергозависимые данные — информация, содержащаяся на энергозависимом носителе информации.

АББРЕВИАТУРЫ

ДБО — дистанционное банковское обслуживание.
ИБ — информационная безопасность.
НЖМД — накопитель на жестких магнитных дисках.
ПО — программное обеспечение.
ЭВМ — электронная вычислительная машина.
CD — компакт-диск.

ПРОБЛЕМАТИКА

В настоящее время наблюдается значительный рост числа фиксируемых в организациях инцидентов, связанных с мошенничеством в системах ДБО. Финансовые потери организации от одного инцидента в системе ДБО составляют от пятисот тысяч рублей до нескольких миллионов рублей (величина нанесенного ущерба зависит от количества денежных средств на счете лица), а риск возникновения данного вида инцидентов не зависит от характера деятельности организации, банка и применяемой системы дистанционного банковского обслуживания, а зависит только от степени защищенности информационной системы организации, соблюдения работниками политики ИБ и пакетом оказываемых банком услуг по контролю за передачей денежных средств клиентов.

Кредитно-финансовые учреждения пытаются снизить количество инцидентов в системах ДБО путем внедрения аппаратных ключей (устройств с неизвлекаемыми криптографическими ключами), создания возможности ограничения доступа в систему ДБО по сетевым адресам и применения систем, идентифицирующих предположительно подложные платежные поручения перед их исполнением, однако злоумышленники применяют и постоянно совершенствуют контрмеры. В частности, для нейтрализации дополнительных мер защиты, вводимых использованием аппаратных ключей и ограничением доступа в систему ДБО по сетевым адресам, злоумышленники формируют, подписывают и передают в банк платежные поручения с использованием клиентских частей систем ДБО, установленных в ЭВМ бухгалтеров, при помощи программных средств удаленного управления компьютерами или используют вредоносное ПО, подменяющее реквизиты легитимного платежного поручения перед подписанием.

ПРИЧИНЫ ИНЦИДЕНТОВ В СИСТЕМАХ ДБО

- Низкий уровень ИБ организаций, халатное отношение к базовым правилам ИБ и рекомендациям банков.
- Возможность получить «легкие деньги» путем хищения денежных средств со счетов физических и юридических лиц.
- Ощущение вседозволенности, безнаказанности у злоумышленников, совершающих хищения денежных средств.
- Доступность вредоносного ПО и сопутствующих услуг, ориентированных на мошенничество в системах ДБО.

НЕОБХОДИМОСТЬ РЕАГИРОВАНИЯ И РАССЛЕДОВАНИЯ

- Во-первых, правильное реагирование на инцидент в системе ДБО позволяет в ряде случаев остановить движение похищенных денежных средств и вернуть их.
- Во-вторых, борьба с мошенничеством в системах ДБО не ограничивается техническими методами и включает в себя не только обеспечение требуемого уровня ИБ в организациях, но и уголовное преследование преступных групп, ответственных за инциденты. Для раскрытия преступлений, связанных с мошенничеством в системах ДБО, необходимо обеспечить технически правильный и юридически значимый сбор материалов, на основе которых будут сформированы доказательства стороны обвинения. К таким материалам относятся машинные носители информации и собственно компьютерная информация организации, в которой произошел инцидент (последующее формирование доказательств производится проведением судебных компьютерных или компьютерно-технических экспертиз).
- В-третьих, неоценима роль расследований в случаях внутренних инцидентов, когда необходимо выявить злоумышленника внутри организации. В этих ситуациях риск повторения инцидента в системе ДБО можно снизить только выявлением лица, ответственного за инцидент.
- В-четвертых, проведенное расследование инцидента в системе ДБО позволяет избежать проблем, возникающих в случае, если во время инцидента ЭВМ организации использовалась в качестве промежуточного сервера для работы в системах ДБО других организаций. В этом случае заключения (отчеты) лиц, проводивших криминалистические исследования в рамках расследования инцидента, позволяют подтвердить непричастность работников к другим инцидентам в системах ДБО.
- В-пятых, зафиксированный в правоохранительных органах факт инцидента в системе ДБО позволяет отчитаться перед налоговыми органами о переводе крупной суммы денежных средств.

ПРИЗНАКИ ИНЦИДЕНТА В СИСТЕМЕ ДБО

- Обнаружение платежных поручений, которые не передавались уполномоченными работниками организации.
- Сообщение из банка, содержащее требование подтвердить исполнение платежных поручений, которые не передавались уполномоченными работниками организации.
- Уменьшение или отсутствие денежных средств на счете при условии, что передача денежных средств не проводилась.
- Невозможность входа в систему ДБО из-за ошибок, достоверно не связанных с техническими проблемами на стороне банка (ошибки аутентификации, возникающие при корректном вводе логина и пароля, недоступность серверов системы ДБО и т. п.).
- Невозможность загрузки операционной системы ЭВМ, на которой работали с системой ДБО[1].

[1] *Т. к. некоторое вредоносное ПО выводит из строя операционную систему компьютера с целью временного сокрытия переданных платежных поручений.*

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ В СИСТЕМЕ ДБО

Включает в себя технические мероприятия, обеспечивающие целостность криминалистически значимых данных и возможность судебного исследования этих данных в будущем, а также организационные мероприятия, которые позволяют снизить ущерб и составить необходимые для правоохранительных органов документы.

Сущностью технических мероприятий является немедленное обеспечение целостности данных, потенциально имеющих отношение к инциденту, путем отключения, упаковки и опечатывания, а затем должного хранения соответствующих носителей информации. Отключение носителей информации позволяет свести к нулю риск уничтожения криминалистически значимых данных в результате работы вредоносных программ и действий злоумышленника, а их упаковка, опечатывание и должное хранение обеспечивают достаточный уровень достоверности результатов криминалистического исследования в суде. Организационные мероприятия заключаются в уведомлении руководства организации, подразделений (служб) информационной безопасности (организации и банка) о факте инцидента, о реквизитах переданных подложных платежных поручений и об иных сведениях технического характера. Документы, составленные при проведении организационных мероприятий, могут использоваться как основания для рассмотрения вопросов о возбуждении уголовных дел или для уточнения вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации организации (при назначении судебных экспертиз для уточнения вопросов эксперту могут использоваться документально подтвержденные реквизиты платежных поручений, переданных во время инцидента: номера платежных поручений, сведения о получателях платежей, назначения платежей).

После реагирования на инцидент в системе ДБО начинается расследование инцидента и восстановление информационной системы организации. Восстановление информационной системы организации заключается в создании новых ключей электронной подписи, предназначенных для работы в системе ДБО, замене изъятых, упакованных и опечатанных носителей информации на новые, установке требуемого ПО и конфигурации информационной системы с учетом повышенных требований ИБ.

ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ

Для проведения технических мероприятий рекомендуется привлекать независимого специалиста, имеющего опыт реагирования на инциденты информационной безопасности, и лиц, не работающих в пострадавшей организации (для удостоверения процесса реагирования). При невозможности привлечения независимого специалиста нижеприведенные мероприятия могут быть проведены работниками подразделений информационной безопасности или иными лицами (системными администраторами), обладающими необходимыми знаниями.

Указанная ниже последовательность действий может быть дополнена другими этапами, предназначенными для обеспечения внутренних расследований.

1. Выявление всех ЭВМ организации, на которых работали с системой ДБО. Составление их списка (в том числе ЭВМ, которые на момент инцидента были выключены).

2. Немедленное выключение работающих ЭВМ из указанного списка методом прерывания электропитания (отключение шнура от блока питания компьютера, снятие аккумуляторной батареи) либо иным методом, обеспечивающим выключение без применения программных средств.

3. Извлечение энергонезависимых носителей информации (НЖМД, флеш-накопители) из ЭВМ, на которых работали с системой ДБО.

4. Упаковка и опечатывание извлеченных носителей информации (правила опечатывания приведены ниже).

5. Упаковка и опечатывание носителей ключевой информации (флеш-накопителей, аппаратных ключей), используемых для подписи платежных поручений.

6. Включение ЭВМ, на которых работали с системой ДБО, без подключения загрузочных носителей информации с целью определения (с помощью интерфейса базовой системы ввода и вывода) и документирования отклонения системных часов компьютера от текущего времени (необязательный шаг).

7. Копирование журналов систем контроля доступа в помещения организации, копирование видеопотока систем видеонаблюдения в офисе или офисном центре за максимально возможный промежуток времени. Запись соответствующих журналов и видеопотоков на компакт-диски, их упаковка и опечатывание.

8. Составление соответствующего акта, в котором отражаются характеристики упакованных и опечатанных носителей и иная значимая информация (пример акта приведен в приложениях).

9. Передача упакованных и опечатанных носителей информации на хранение в специальном помещении или сейфе.

ОБЕСПЕЧЕНИЕ СЛУЖЕБНЫХ РАССЛЕДОВАНИЙ

При необходимости проведения внутреннего (служебного) расследования инцидента в системе ДБО следует создать копии содержимого энергонезависимых носителей информации ЭВМ, на которых работали с системой ДБО, скопировать значимые лог-файлы сетевого оборудования организации и запросить статистику сетевых взаимодействий у интернет-провайдера организации и журналы работы в системе ДБО у банка, также рекомендуется сделать копию сетевого трафика, передаваемого в локальной вычислительной сети организации в момент реагирования на инцидент. Основным источником криминалистически значимых данных являются энергонезависимые носители информации (НЖМД, флеш-накопители), поэтому исследование их содержимого носит ключевой характер. Исследование других видов данных (копий содержимого оперативной памяти, копий сетевого трафика, лог-файлов) без исследования содержимого энергонезависимых носителей информации нельзя признать достаточным.

В некоторых случаях целесообразно создавать копии содержимого энергозависимых носителей информации (оперативной памяти) ЭВМ, на которых работали с системой ДБО, до их выключения, а также проводить копирование содержимого энергонезависимых носителей информации без выключения ЭВМ (например, если данные ЭВМ являются критически важными серверами организации, выключение которых приведет к нарушению бизнес-процессов). В этих случаях нужно помнить, что копирование данных на работающей системе путем запуска специализированных программ приводит к существенному изменению состояния ЭВМ (созданию новых файлов и ключей реестра, изменению временных меток файлов и директорий, изменению файла подкачки Windows и т. д.), может привести к запуску так называемых «логических бомб», что в итоге может негативно отразиться на оценке достоверности последующих результатов криминалистических исследований, поэтому проведение подобных действий требует подробного документирования (указания времени начала и окончания соответствующих действий, используемых программ, сведений о выводимых ошибках и предупреждениях и др.).

При сборе какой-либо информации на работающей системе нельзя создавать копии данных (копии содержимого оперативной памяти, копии содержимого энергонезависимых носителей информации) на

носителях информации, используемых в составе ЭВМ. Для записи этих копий следует использовать внешние носители информации достаточной емкости, не имеющие отношения к инциденту (НЖМД, подключаемые к ЭВМ по интерфейсу USB и т. п.).

КОПИРОВАНИЕ СОДЕРЖИМОГО ЭНЕРГОНЕЗАВИСИМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Для внутренних расследований инцидентов следует создавать криминалистические образы (копии содержимого) энергонезависимых носителей информации перед их упаковкой и опечатыванием. Полученные образы могут использоваться для проведения внесудебных криминалистических исследований, а упакованные и опечатанные носители информации при необходимости могут быть переданы в правоохранительные органы для приобщения к материалам проверки (или к материалам уголовного дела в порядке, предусмотренном частью 2 статьи 86 Уголовно-процессуального кодекса РФ) и для проведения судебной экспертизы в рамках уголовного дела. Создание таких образов целесообразно проводить с использованием программ dd и dc3dd на специализированных загрузочных компакт-дисках на основе Linux, которые позволяют работать с подключенными энергонезависимыми носителями информации в режиме «только чтение».

Если работа с системой ДБО проводилась с использованием ЭВМ, выключение которых по каким-либо причинам невозможно, то следует создать криминалистические образы их энергонезависимых носителей информации на работающей системе с использованием рекомендуемых специализированных программных средств для операционных систем семейства Windows. Созданные криминалистические образы нужно записать на два комплекта носителей информации, один из которых следует опечатать и передать на должное хранение, а второй использовать для проведения внутренних расследований. Упакованные и опечатанные носители информации, содержащие криминалистические образы, при необходимости могут быть переданы в правоохранительные органы для приобщения к материалам проверки (или к материалам уголовного дела в порядке, предусмотренном частью 2 статьи 86 Уголовно-процессуального кодекса РФ) и для проведения судебной экспертизы в рамках уголовного дела.

РЕКОМЕНДУЕМОЕ ПО
RIP Linux: www.tux.org/pub/people/kent-robotti/looplinux/rip/
CAINE Live CD: www.caine-live.net
FTK Imager Lite: www.accessdata.com/support/adownloads
dd для Windows: www.chrysocome.net/dd, www.gmgsystemsinc.com/fau/

КОПИРОВАНИЕ ЭНЕРГОЗАВИСИМЫХ ДАННЫХ, ЛОГ-ФАЙЛОВ СЕТЕВОГО ОБОРУДОВАНИЯ И СЕТЕВОГО ТРАФИКА

Перед выключением работающих ЭВМ, имеющих отношение к инциденту в системе ДБО, а также перед созданием криминалистических образов энергонезависимых носителей информации на работающих ЭВМ, выключение которых по каким-либо причинам невозможно, возможно создание копий содержимого оперативной памяти компьютеров с использованием рекомендуемого программного обеспечения. При проведении криминалистических исследований копии содержимого оперативной памяти могут использоваться для обнаружения следов работы вредоносных программ (в том числе работающих исключительно в энергозависимой памяти ЭВМ) и следов системной активности злоумышленника.

После создания копии содержимого оперативной памяти ее нужно записать (в виде файла или нескольких файлов) на два компакт-диска, один из которых следует упаковать, опечатать и передать на должное хранение, а второй использовать для проведения внутренних (служебных) расследований. Упакованный и опечатанный компакт-диск при необходимости может быть передан в правоохранительные органы для приобщения к материалам проверки (или к материалам уголовного дела в порядке, предусмотренном частью 2 статьи 86 Уголовно-процессуального кодекса РФ) и для проведения судебной экспертизы в рамках уголовного дела.

РЕКОМЕНДУЕМОЕ ПО
win32dd (win64dd): www.moonsols.com/windows-memory-toolkit/
FTK Imager Lite: www.accessdata.com/support/adownloads

Для увеличения вероятности успешного расследования инцидента в системе ДБО следует сделать копию сетевого трафика, передаваемого в локальной вычислительной сети организации в момент реагирования на инцидент, а также создать копии лог-файлов сетевого оборудования организации (прокси-серверов, ретрансляторов сетевых адресов и портов, систем обнаружения вторжений и др.) за соответствующий временной промежуток (за два или три месяца до даты инцидента по настоящее время). Копии сетевого трафика и лог-файлов нужно записать на два комплекта компакт-дисков, один из которых следует опечатать и передать на должное хранение (для передачи в правоохранительные органы при необходимости), а второй использовать для проведения внутренних (служебных) расследований.

Копирование сетевого трафика в файл рекомендуется проводить с помощью программных средств, указанных ниже. При этом необходимо копировать сетевой трафик в определенной точке локальной

вычислительной сети, обеспечивающей перехват криминалистически значимых потоков данных (т. е. потоков данных из сегмента вычислительной сети, в котором произошел инцидент).

Копирование лог-файлов сетевого оборудования рекомендуется проводить путем экспорта соответствующих типов данных (журналов доступа, журналов сетевых событий и т. п.) из интерфейса управления устройством на сменный носитель. К сожалению, из-за большого количества видов, моделей сетевого оборудования и разнообразия способов управления ими невозможно дать конкретные инструкции по экспорту криминалистически значимых данных на сменные носители. В каждом конкретном случае следует обращаться к документации сетевого оборудования.

РЕКОМЕНДУЕМОЕ ПО

tcpdump: www.tcpdump.org
Wireshark: www.wireshark.org

ЗАПРОС ЛОГ-ФАЙЛОВ У ИНТЕРНЕТ-ПРОВАЙДЕРА

Для проведения внутренних (служебных) расследований целесообразно запросить журналы сетевых взаимодействий (подключений) у интернет-провайдера организации за определенный период времени (за два или три месяца до даты инцидента по настоящее время). Пример запроса приведен в приложениях.

Следует учитывать, что некоторые интернет-провайдеры не предоставляют собственным клиентам статистику их сетевых подключений (а предоставляют ее только по запросу правоохранительных органов).

ЗАПРОС ЛОГ-ФАЙЛОВ СИСТЕМЫ ДБО У БАНКА

Для проведения внутренних (служебных) расследований целесообразно запросить журналы работы учетной записи организации в системе ДБО у банка за определенный период времени (за два или три месяца до даты инцидента по настоящее время). Пример запроса приведен в приложениях.

Следует учитывать, что некоторые банки не предоставляют собственным клиентам соответствующие журналы (а предоставляют их только по запросу правоохранительных органов).

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ

Рекомендуемая последовательность действий, составляющих организационную основу на инцидент в системе ДБО. Действия следует проводить параллельно с техническими мероприятиями.

1. Немедленно сообщить по телефону в подразделение информационной безопасности банка о факте несанкционированной передачи платежных поручений с указанием их реквизитов: номеров, сумм, получателей, назначений платежей. Потребовать отмены указанных платежных поручений и аннулирования действующего сертификата ключа электронной подписи организации.

2. Оформить докладную записку руководителю организации о факте инцидента с указанием реквизитов переданных платежных поручений (пример докладной записки приведен в приложениях).

3. Подготовить документы для правоохранительных органов и работников банка (описание инцидента в письменной форме, договор на предоставление услуги ДБО, договор на предоставление услуги доступа в сеть Интернет, копии несанкционированных платежных поручений, заявление о преступлении). Примерный перечень вопросов, на которые необходимо дать ответ при составлении подробного описания инцидента, дан в приложениях. Заявление о преступлении оформляется с учетом требований статьи 141 Уголовно-процессуального кодекса РФ и передается в орган МВД России для регистрации[1] и последующей проверки.

[1] *Если заявление о преступлении передается при личном обращении заявителя, то ему выдается талон-уведомление (пункт 68 приложения к приказу МВД России от 01.03.2012 №140).*

ПРАВИЛА УПАКОВКИ И ОПЕЧАТЫВАНИЯ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Способ опечатывания машинных носителей информации должен обеспечивать невозможность доступа к носителю без видимого нарушения целостности упаковки.

Наиболее простым допустимым способом упаковки и опечатывания НЖМД, флеш-накопителей и других объектов небольшого размера является их помещение в полиэтиленовый пакет с последующей перевязкой его горловины нитью, на концы которой наклеивается пояснительная записка с подписями участвующих в опечатывании лиц и печатью организации.

Порядок перевязки горловины пакета нитью: длинной нитью обвязать горловину пакета двумя последовательностями витков (интервал между последовательностями витков: от 5 до 10 мм), после каждой последовательности витков нить следует завязать узлом, в процессе перевязки нить не разрывать.

После перевязки горловины пакета концы нити следует пропустить по внутренней линии сгиба прямоугольного листа бумаги, сложенного пополам. Лист, сложенный пополам, нужно склеить. Оба конца нити следует приклеить с помощью двух небольших фрагментов бумаги к сложенному прямоугольному листу бумаги. Далее на участки склеивания следует нанести подписи участвующих лиц и печати.

ОШИБКИ ПРИ РЕАГИРОВАНИИ НА ИНЦИДЕНТ В СИСТЕМЕ ДБО

- Антивирусная проверка файловых систем носителей информации ЭВМ, на которых работали в системе ДБО, после обнаружения инцидента (приводит к изменению временных меток файлов вредоносных программ, перемещению или удалению файлов вредоносных программ).
- Переустановка операционных систем ЭВМ, на которых работали в системе ДБО, после обнаружения признаков инцидента (приводит к удалению файлов вредоносных программ, следов их работы и усложняет расследование инцидента за счет необходимости восстановления данных).

- Продолжение работы пользователей с ЭВМ, имеющими отношение к инциденту, после обнаружения инцидента; необоснованный перенос выключения ЭВМ на более поздний срок (дает возможность злоумышленнику удалить следы собственной активности).
- Несвоевременное информирование подразделения информационной безопасности банка о факте несанкционированной передачи платежных поручений (приводит к исполнению платежных поручений, переданных злоумышленником, а также к возможности передачи новых платежных поручений с помощью скопированных злоумышленником ключей электронной подписи).
- Необоснованное отклонение от рекомендуемой последовательности действий, зафиксированной в данной инструкции; медленное реагирование на инцидент (приводит к снижению юридической значимости собираемых материалов, перезаписи криминалистически значимых данных).

ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТ В СИСТЕМЕ ДБО НИ В КОЕМ СЛУЧАЕ НЕ ДОЛЖЕН ДОПУСКАТЬ СОВЕРШЕНИЯ ВЫШЕУКАЗАННЫХ ОШИБОК

ПРЕДУПРЕЖДЕНИЕ ИНЦИДЕНТОВ

После завершения процесса реагирования на инцидент в системе ДБО необходимо проверить выполнение нижеуказанного перечня мер, позволяющих существенно снизить вероятность повторения инцидента. Следует незамедлительно обеспечить исполнение всех перечисленных мер безопасности, выполняемых не в полном объеме, а также мер безопасности, описанных в документации банка.

Меры по защите носителей ключей электронной подписи, используемых для работы в системе ДБО:

- носители следует хранить в защищенных местах (сейфах);
- носители должны использоваться только уполномоченными лицами;
- запрещено передавать носитель одного уполномоченного лица другому уполномоченному лицу;
- запрещено устанавливать носители в компьютеры, не используемые для работы в системе ДБО;
- запрещено оставлять носители установленными в компьютерах после завершения сеанса работы в системе ДБО;
- запрещено изготавливать копии криптографических ключей, используемых для работы в системе ДБО, без санкции уполномоченных лиц;
- запрещено хранить резервные и рабочие копии файлов криптографических ключей, используемых для работы в системе ДБО, на любых компьютерах организации, а также на каких-либо машинных носителях вне защищенных мест (сейфов).

Меры по обеспечению ИБ компьютеров, используемых для работы в системе ДБО:

- компьютеры, применяемые для работы в системе ДБО, не должны использоваться в каких-либо других целях, даже рабочих;
- следует регулярно обновлять все программное обеспечение, установленное на компьютерах;
- на компьютерах должно быть установлено антивирусное ПО;
- обновление антивирусного программного обеспечения следует производить не реже раза в сутки;
- не реже раза в неделю следует производить полное антивирусное сканирование машинных носителей информации компьютеров;
- работа на компьютере должна производиться с использованием учетной записи с ограниченными правами, доступ к учетной записи с полными правами должен быть защищен надежным паролем;
- сетевое оборудование, обеспечивающее доступ организации в сеть Интернет, должно блокировать любые сетевые пакеты, передаваемые с компьютера, применяемого для работы в системе ДБО, на серверы, не относящиеся к системе ДБО, веб-сайту банка, службам обновления установленного программного обеспечения и антивирусных баз.

Вышеуказанный перечень мер безопасности может использоваться для разработки общих правил безопасной работы в системах ДБО.

ЗАКЛЮЧЕНИЕ

Для выполнения рекомендаций настоящей инструкции лица, в служебные обязанности которых входит реагирование на инциденты ИБ, должны:

- знать общие правила реагирования на инциденты в системах ДБО и правила сбора материалов (машинных носителей информации и компьютерной информации);
- знать последовательность технических и организационных действий по реагированию на инциденты в системах ДБО;
- уметь работать с программными средствами, указанными в списках рекомендуемого ПО.

Следует помнить, что ущерб от инцидента в системе ДБО, затраты на реагирование на этот инцидент и его расследование превышают затраты на обеспечение требуемого уровня ИБ, необходимого для предотвращения инцидентов в системах ДБО. Соблюдение работниками организации действующей политики ИБ, наличие современных технических средств защиты информации (антивирусное ПО, межсетевые экраны и т. д.), грамотная настройка правил разрешенных сетевых взаимодействий ЭВМ, используемых для работы в системе ДБО, позволяют существенно снизить риск возникновения инцидента в системе ДБО.

ПРИЛОЖЕНИЯ

ОБРАЗЦЫ ДОКУМЕНТОВ

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ОПИСАНИЯ ИНЦИДЕНТА

РУКОВОДСТВА ПО СОЗДАНИЮ КРИМИНАЛИСТИЧЕСКИХ ОБРАЗОВ

РУКОВОДСТВО ПО КОПИРОВАНИЮ СОДЕРЖИМОГО ОПЕРАТИВНОЙ ПАМЯТИ

ОБРАЗЦЫ ДОКУМЕНТОВ

АКТ ОБ ИЗЪЯТИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ

10 марта 2011 года в офисе ООО «Вектор», расположенном по адресу: г. Москва, ул. Ленина, д, 10, строение 3, в присутствии следующих лиц:

1. Иванов И. И. (генеральный директор ООО «Вектор»)
2. Петров П. П. (системный администратор ООО «Вектор»)
3. Сидоров С. С. (независимое лицо, привлеченное для удостоверения проводимых действий)
4. Гусева Г. Г. (независимое лицо, привлеченное для удостоверения проводимых действий)

специалистом ЗАО «Расследование инцидентов» Черных Д.С. было произведено изъятие носителей информации и копирование их содержимого с целью дальнейшего исследования.

Были изъяты следующие носители информации:
1. накопитель на жестких магнитных дисках из компьютера бухгалтерии ООО «Вектор» (производитель: «Seagate», модель: «ST3120022A», серийный номер: «5JS4JNCC», заявленная емкость: 120 Гбайт);
2. накопитель USB Flash «Transcend JF V30 / 1 GB» из помещения бухгалтерии ООО «Вектор».
Содержимое изъятых носителей информации было скопировано на накопитель на жестких магнитных дисках специалиста (производитель: «Western Digital», модель: «WD20EADS-00H7B0», серийный номер: «WCAUP0016286», заявленная емкость: 2 Тбайта).
После копирования изъятые носители информации были упакованы и опечатаны способом, обеспечивающим невозможность доступа к носителю без видимого нарушения целостности упаковки.

Специалист ЗАО «Расследование инцидентов» Черных Д. С.
(подпись)
Генеральный директор ООО «Вектор» Иванов И. И.
(подпись)
Системный администратор ООО «Вектор» Петров П. П.
(подпись)
Независимое лицо Сидоров С. С.
(подпись)
Независимое лицо Гусева Г. Г.
(подпись)

10.03.2011

ДОКЛАДНАЯ ЗАПИСКА РУКОВОДИТЕЛЮ ОРГАНИЗАЦИИ

Генеральному директору
ООО «Вектор»
И. И. Иванову

ДОКЛАДНАЯ ЗАПИСКА
№43 ОТ 09.04.2011

9 апреля 2011 года в 10:35 главным бухгалтером П. П. Петровой в системе дистанционного банковского обслуживания, предоставляемой ОАО «Вектор-банк», были обнаружены платежные поручения №141, №142 и №143 на общую сумму один миллион двести тысяч пятьсот тридцать один рубль 00 копеек, которые не передавались в банк работниками бухгалтерии.

Указанные платежные поручения в поле «назначение платежа» содержат ссылки на не зарегистрированные, согласно сведениям, полученным от П. П. Петровой, в нашей организации договоры аренды помещений и покупки пропиленовых труб.

На основании вышеизложенного я расцениваю передачу указанных платежных поручений как инцидент информационной безопасности и немедленно приступаю к реагированию на него с целью предотвращения повторения инцидента и сбора криминалистически значимых данных для выявления причин возникновения инцидента.

Прошу рассмотреть вопрос о целесообразности обращения в правоохранительные органы и привлечении сторонних специалистов для проведения служебного расследования и выявления причастных к инциденту лиц.

Распечатанные П. П. Петровой платежные поручения №141, №142 и №143 приложены к служебной записке.

Системный администратор
(подпись)
С. С. Сидоров

ДОКЛАДНУЮ ЗАПИСКУ СЛЕДУЕТ ОФОРМИТЬ СОГЛАСНО ПРИНЯТЫМ В ОРГАНИЗАЦИИ ТРЕБОВАНИЯМ К СОСТАВЛЕНИЮ ДОКУМЕНТОВ

ЗАПРОС ЛОГ-ФАЙЛОВ У ИНТЕРНЕТ-ПРОВАЙДЕРА

ЗАПРОС ИНФОРМАЦИИ

Просим вас предоставить статистику сетевых взаимодействий с IP-адресом 101.22.240.12, который используется маршрутизатором в локальной вычислительной сети ООО «Вектор», за период с 1 марта 2011 года по 15 мая 2011 года в связи с проводимым служебным расследованием инцидента информационной безопасности.

Договор на оказание услуг связи №1241 от 9 июня 2010 года.

Главный специалист отдела безопасности ООО «Вектор»
(подпись)
И. И. Иванов

ЗАПРОС СЛЕДУЕТ ОФОРМИТЬ СОГЛАСНО ПРИНЯТЫМ В ОРГАНИЗАЦИИ ТРЕБОВАНИЯМ К СОСТАВЛЕНИЮ ДОКУМЕНТОВ С УЧЕТОМ СПОСОБА ПЕРЕДАЧИ ЗАПРОСА

ЗАПРОС ЛОГ-ФАЙЛОВ У БАНКА

ЗАПРОС ИНФОРМАЦИИ

Просим вас предоставить записи о событиях работы в системе дистанционного банковского обслуживания для учетной записи ООО «Вектор» (логин: «vector-1936») за период с 1 февраля 2011 года по 12 апреля 2011 года в связи с проводимым служебным расследованием инцидента информационной безопасности, связанного с несанкционированной передачей платежных поручений.

Договор на оказание услуг №1936 от 19 сентября 2010 года.

Главный специалист отдела безопасности ООО «Вектор»
(подпись)
И. И. Иванов

ЗАПРОС СЛЕДУЕТ ОФОРМИТЬ СОГЛАСНО ПРИНЯТЫМ В ОРГАНИЗАЦИИ ТРЕБОВАНИЯМ К СОСТАВЛЕНИЮ ДОКУМЕНТОВ С УЧЕТОМ СПОСОБА ПЕРЕДАЧИ ЗАПРОСА

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ СОСТАВЛЕНИЯ ОПИСАНИЯ ИНЦИДЕНТА

- Когда и как вы обнаружили передачу несанкционированных (мошеннических) платежных поручений?
- Отображались ли вам какие-нибудь необычные сообщения при работе с системой ДБО непосредственно до инцидента (сообщения о технических работах, об ошибках)? Если да, то какие это были сообщения?
- Замечали ли вы какие-нибудь необычные события при работе с компьютером непосредственно до инцидента (беспричинные движения курсора мыши, ввод текста, запуск программ)? Если да, то какие это были события?
- Поступали ли вам звонки от лиц, представившихся работниками банка, непосредственно до инцидента? Если да, то о чем вы говорили?
- Какие виды носителей ключей электронной подписи используются (дискеты, флеш-накопители, аппаратные ключи)?
- Какие носители ключей электронной подписи необходимы для корректного подписания платежного поручения? За какими лицами они закреплены?
- Как организована работа с носителями ключей электронной подписи? Как и где они хранятся в нерабочее (ночное, обеденное) время? Какие лица имеют к ним доступ?
- Принято ли в организации передавать свой ключ электронной подписи другому лицу?
- Как организовано хранение резервных копий ключей электронной подписи? Какие лица имеют к ним доступ?
- Какие действия производились с носителями ключей электронной подписи и их резервными копиями непосредственно до инцидента?
- Применяется ли компьютер в целях, отличных от работы в системе ДБО? Если да, то в каких?

- Как часто производится обновление программного обеспечения, установленного на компьютере? Когда было последнее обновление?
- Какие антивирусные программы установлены на компьютере? Как часто они обновляются?
- Какие программные межсетевые экраны установлены на компьютере? Какие правила сетевых взаимодействий они реализуют?
- Какие программные средства удаленного (сетевого) управления установлены на компьютере? Для каких целей они используются?
- Производилось ли антивирусное сканирование компьютера после обнаружения инцидента? Если да, то какие оно дало результаты?
- Производилась ли переустановка операционной системы компьютера после обнаружения инцидента?
- Как организован доступ организации в сеть интернет? Какие правила сетевых взаимодействий реализуются межсетевыми экранами? При ответе на этот вопрос желательно нарисовать карту сети.
- Установлена ли в офисе система контроля и управления доступом в помещения? Если да, то ведет ли она журналы доступа?
- Ведется ли в офисе или бизнес-центре видеонаблюдение? Как долго хранится видеоряд?

РУКОВОДСТВО ПО СОЗДАНИЮ КРИМИНАЛИСТИЧЕСКИХ ОБРАЗОВ С ПОМОЩЬЮ FTK IMAGER LITE (НА РАБОТАЮЩЕЙ СИСТЕМЕ)

1. Файлы программного продукта FTK Imager Lite следует записать на сменный носитель информации, который будет подключаться к работающим ЭВМ под управлением операционных систем семейства Windows. Во избежание распространения вредоносных программ через сменные носители информации рекомендуется использовать носители однократной записи (компакт-диски).

2. Подключить к ЭВМ сменный носитель информации, на котором будет создан образ. В качестве такого носителя информации можно использовать внешний НЖМД, подключаемый к ЭВМ по интерфейсу USB. Подключаемый сменный носитель информации следует предварительно отформатировать в файловую систему NTFS.

3. После подключения сменного носителя информации с записанным программным обеспечением FTK Imager Lite к ЭВМ запустить исполняемый файл с именем «FTK Imager.exe» с правами администратора.

4. После загрузки программы появится окно (*рис. 1*).

5. Выбрать пункт меню «File — Create Disk Image...». Будет отображено окно выбора типа источника данных (*рис. 2*).

6. Далее следует выбрать требуемый тип источника данных. В качестве источника данных могут выступать «физические диски» (содержимое носителя информации, непосредственно доступное для операционной системы, включает в себя таблицу разделов, области данных вне разделов и файловые системы) и «логические диски» (содержимое определенной файловой системы или определенного раздела). В большинстве случаев целесообразно в качестве типа источника выбирать «физический диск», выбор «логического диска» рекомендуется в следующих случаях:

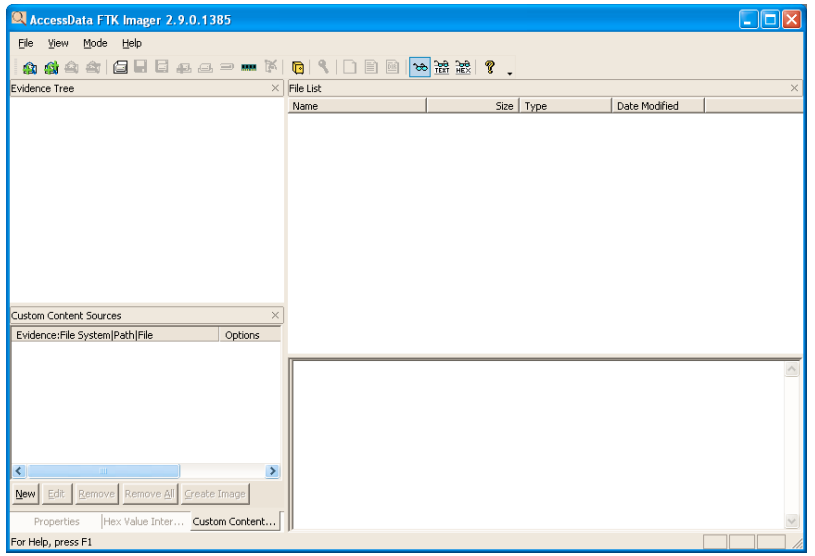

Рисунок 1. *Главное окно программы FTK Imager Lite*

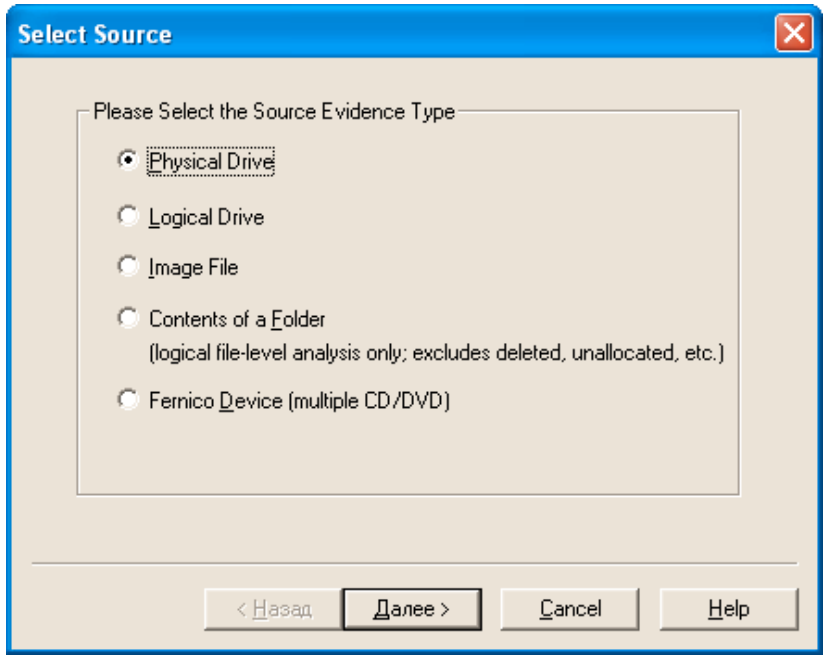

Рисунок 2. *Окно выбора типа источника данных*

- носители информации в ЭВМ образуют программный отказоустойчивый массив (RAID), а данные следует скопировать в декодированном виде (для исключения дальнейшей сборки массива);

- используется программное шифрование всего содержимого носителей информации в ЭВМ (полнодисковое шифрование), а данные следует скопировать в расшифрованном виде.

ПОСЛЕ ВЫБОРА ТИПА ИСТОЧНИКА ДАННЫХ НАЖАТЬ КНОПКУ «ДАЛЕЕ».

7. После выбора типа источника данных следует выбрать источник данных (устройство, соответствующее требуемому носителю информации; для «логических дисков», «букву диска»). После выбора источника данных нажать кнопку «Finish» (*рис. 3 и 4*).

8. Отображается общее окно параметров создаваемых образов, (*рис. 5*). В указанном окне следует нажать кнопку «Add...».

9. Отображается окно выбора типа создаваемого образа. В указанном окне рекомендуется выбрать «Raw (dd)» (точная копия данных без сжатия или шифрования) и нажать кнопку «Далее» (*рис. 6*).

10. В окне ввода дополнительной информации (*рис. 7*) поля ввода текстовой информации не являются обязательными к заполнению. Рекомендуется ввести фамилию человека, создающего криминалистический образ (поле «Examiner»), и сведения, указывающие на ЭВМ, образы носителей информации которой создаются (поле «Notes»). После ввода информации нажать кнопку «Далее».

11. В окне ввода параметров создаваемого образа следует выбрать директорию, в которой будет создан образ носителя информации в виде файла (или нескольких файлов), ввести шаблон имен файлов-образов без расширения и выбрать размер фрагментов образа (для создания образа в виде нескольких файлов, размер которых равен заданному или не превышает его). При создании образов на сменных носителях, отформатированных в файловую систему NTFS, ограничения на максимальный размер файлов превышают емкость современных носителей информации, поэтому в качестве размера фрагмента рекомендуется указывать «0» (образ будет создан в виде одного файла). После ввода требуемых данных следует нажать кнопку «Finish».

После выбора директории для сохранения создаваемого образа следует убедиться, что выбранная директория соответствует подключенному при выполнении пункта 2 сменному носителю информации (рис. 8)!

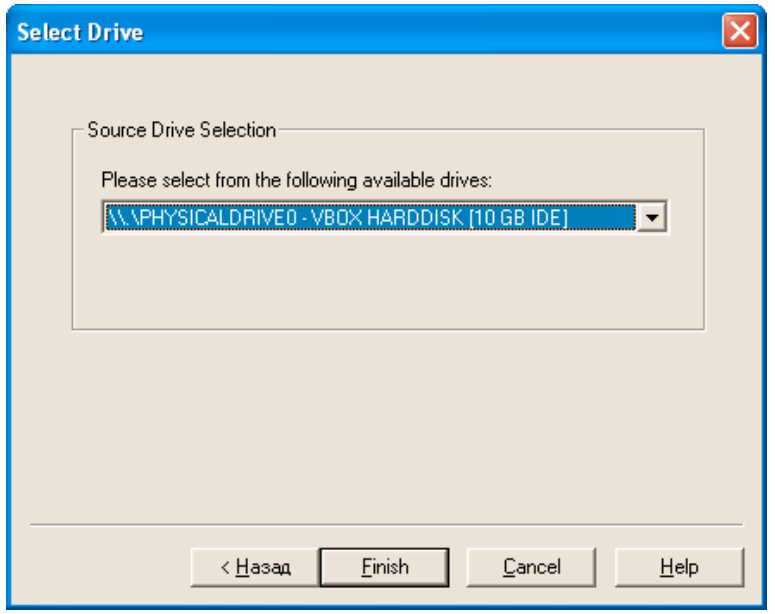

Рисунок 3. *Выбор «физического диска»*

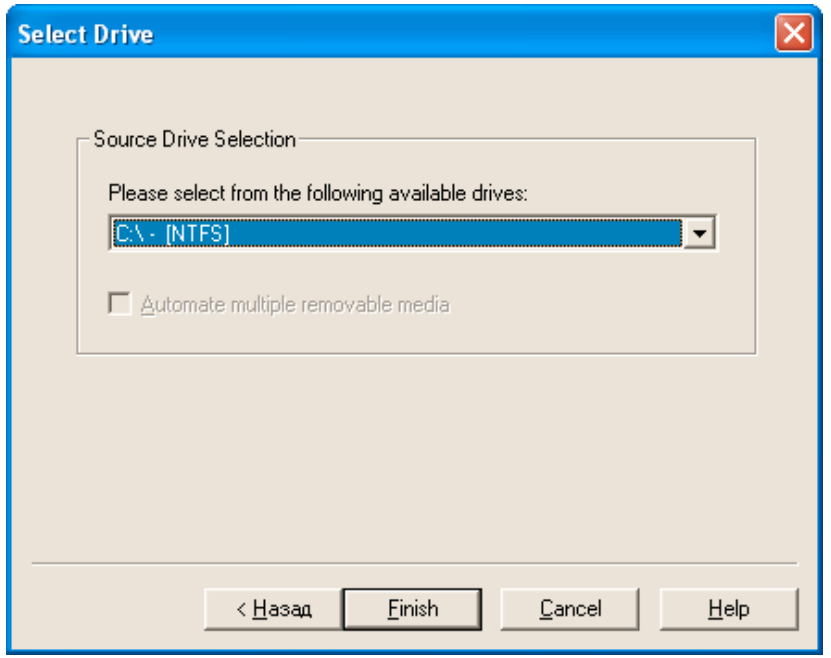

Рисунок 4. *Выбор «логического диска»*

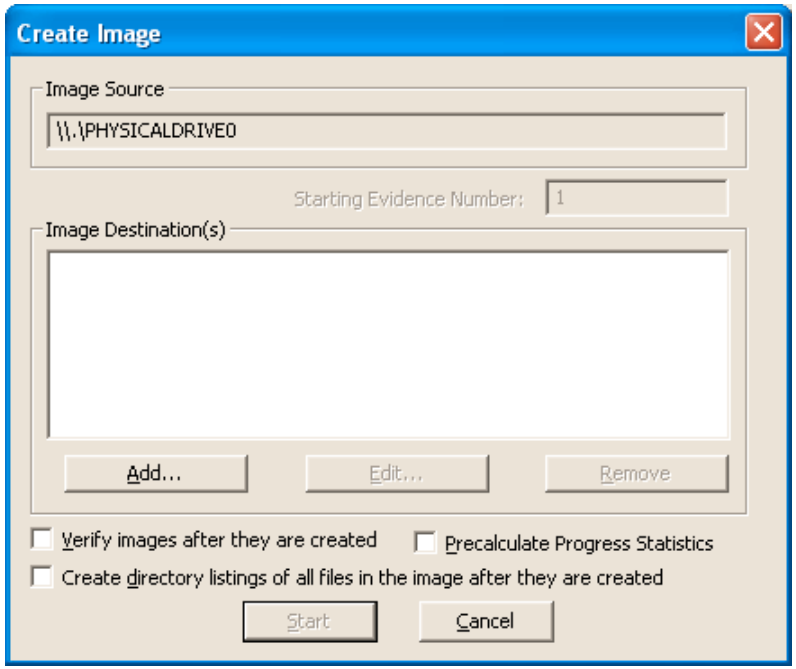

Рисунок 5. Общее окно параметров создаваемых образов

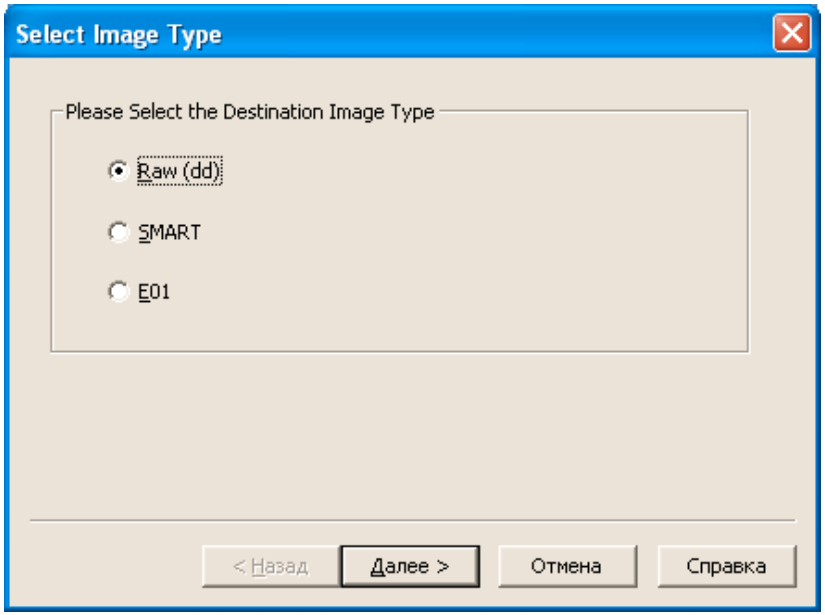

Рисунок 6. Окно выбора типа создаваемого образа

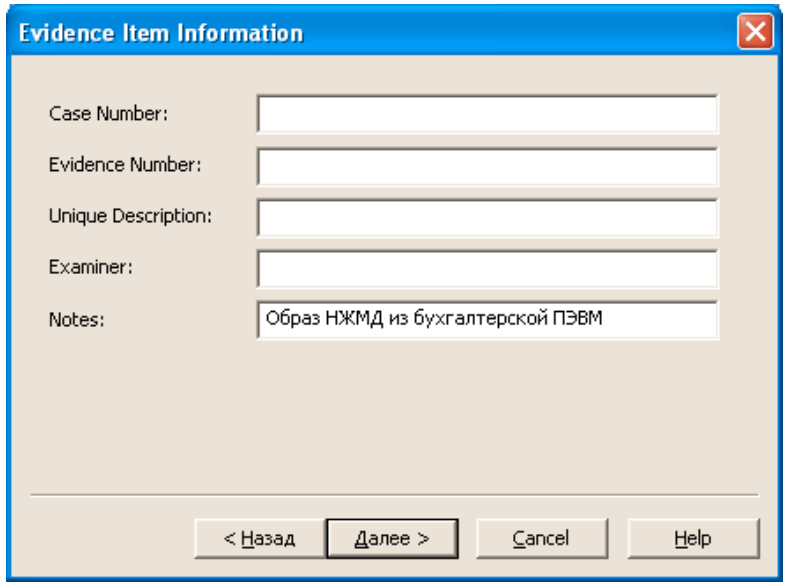

Рисунок 7. Окно ввода дополнительной информации

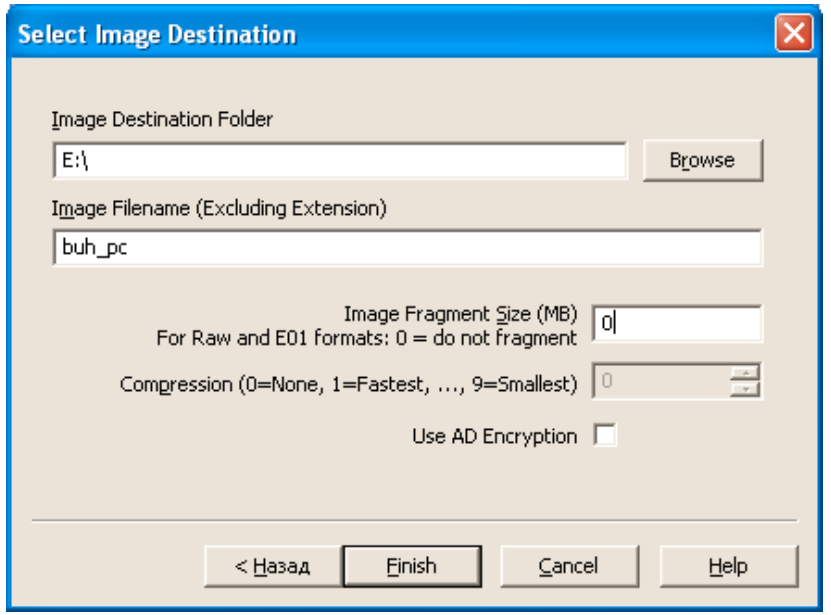

Рисунок 8. Окно ввода параметров создаваемого образа

12. Далее будет отображено общее окно параметров создаваемых образов. В указанном окне следует снять пометки со всех трех пунктов выбора и нажать кнопку «Start» (*рис. 9*).

13. Будет запущен процесс копирования данных, состояние которого отображается в статусных окнах, представленных ниже. После завершения копирования в поле «Status» будет отображена строка «Image created successfully» (*рис. 10 и 11*).

14. В директории, выбранной для сохранения создаваемого образа, будут записаны два файла (если был создан нефрагментированный образ): файл-образ и текстовый файл, содержащий дополнительную информацию.

15. При необходимости создать криминалистические образы других энергонезависимых носителей информации из состава ЭВМ.

16. Закрыть программу FTK Imager Lite, отключить сменный носитель информации, на котором был создан образ, извлечь сменный носитель с программным обеспечением FTK Imager Lite.

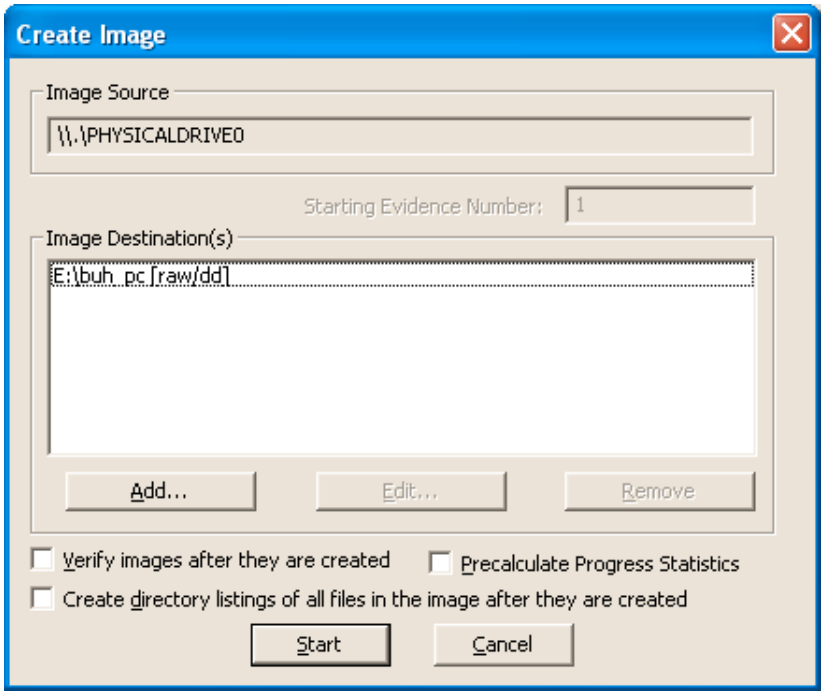

Рисунок 9. *Общее окно параметров создаваемых образов*

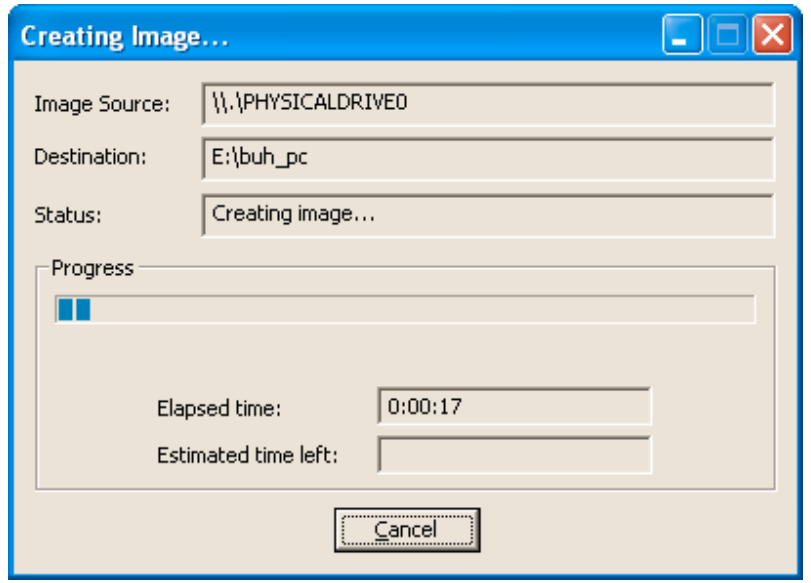

Рисунок 10. *Статусное окно в процессе копирования*

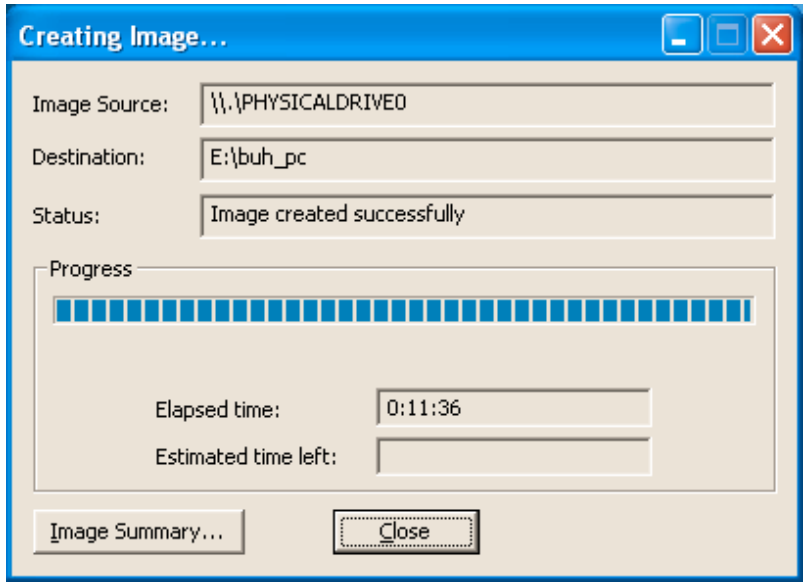

Рисунок 11. *Статусное окно после завершения копирования*

РУКОВОДСТВО ПО КОПИРОВАНИЮ СОДЕРЖИМОГО ОПЕРАТИВНОЙ ПАМЯТИ С ПОМОЩЬЮ ПРОГРАММЫ WIN32DD (НА РАБОТАЮЩЕЙ СИСТЕМЕ)

1. Файлы программного продукта MoonSols Windows Memory Toolkit (Community Edition) следует записать на сменный носитель информации, который будет подключаться к работающим ЭВМ под управлением операционных систем семейства Windows. Во избежание распространения вредоносных программ через сменные носители информации рекомендуется использовать носители однократной записи (компакт-диски).

2. Подключить к ЭВМ сменный носитель информации, на котором будет создан образ оперативной памяти. В качестве такого носителя информации можно использовать внешний НЖМД, подключаемый к ЭВМ по интерфейсу USB, или накопитель типа USB Flash достаточной емкости. Подключаемый сменный носитель информации следует предварительно отформатировать в файловую систему NTFS.

3. После подключения сменного носителя информации с записанным программным обеспечением MoonSols Windows Memory Toolkit (Community Edition) к ЭВМ запустить системный интерпретатор командной строки с правами администратора (программа «cmd.exe»). В русскоязычных версиях операционной системы Windows XP для запуска интерпретатора командной строки нажать кнопку «Пуск» и выбрать следующий пункт меню: «Все программы — Стандартные — Командная строка», либо нажать кнопку «Пуск», выбрать пункт меню «Выполнить...», ввести в отображаемом окне «Запуск программы» в поле «Открыть» текст «cmd» (без кавычек) и нажать кнопку «ОК».

4. После запуска интерпретатора командной строки перейти в директорию с записанным программным обеспечением MoonSols Windows Memory Toolkit (Community Edition). Если сменный носитель с данным программным обеспечением был подключен к системе как «диск E:», а файлы программного обеспечения

записаны в директории «moonsols_windows_memory_toolkit_community_edition» в корне файловой системы этого носителя, то следует ввести следующие команды (после ввода каждой команды следует нажимать клавишу «Enter»):

- E:
- cd moonsols_windows_memory_toolkit_community_edition

Смену текущего диска следует производить вводом буквы требуемого диска с двоеточием, а смену текущей директории в рамках текущего диска — командой «cd» с указанием требуемой директории в качестве параметра.

5. Запустить программу win32dd следующей командой:
- win32dd.exe /f E:\ram-image.dd

Где: «E:\ram-image.dd» — адрес файла, в который будет скопировано текущее содержимое оперативной памяти ЭВМ (файл должен создаваться на сменном носителе, подключенном при выполнении пункта 2).

6. На запрос программы win32dd с текстом «--> Are you sure you want to continue? [y/n]» ввести «y» (без кавычек) и нажать клавишу «Enter».

7. После завершения процесса копирования в текстовом выводе программы будет строка «Processing....Done.».

8. Закрыть интерпретатор командной строки, отключить сменный носитель информации, на котором был создан криминалистический образ оперативной памяти, средствами операционной системы, извлечь сменный носитель с программным обеспечением MoonSols Windows Memory Toolkit (Community Edition).

ВЫВОД ПРОГРАММЫ WIN32DD ПОСЛЕ СОЗДАНИЯ ОБРАЗА ОПЕРАТИВНОЙ ПАМЯТИ

```
win32dd - 1.3.1.20100417 - (Community Edition)
Kernel land physical memory acquisition
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Name            Value
----            -----
File type:         Raw memory dump file
Acquisition method:     PFN Mapping
Content:          Memory manager physical memory block

Destination path:      E:\ram-image.dd

O.S. Version:        Microsoft Windows XP Professional Service Pack 3
(build 2600)
Computer name:       35DC2F12CCCD40E

Physical memory in use:     42%
Physical memory size:    523760 Kb (  511 Mb)
Physical memory available:  301908 Kb (  294 Mb)

Paging file size:      788528 Kb (  770 Mb)
Paging file available:    606804 Kb (  592 Mb)

Virtual memory size:    2097024 Kb (  2047 Mb)
Virtual memory available:  2083452 Kb (  2034 Mb)

Extented memory available:    0 Kb (   0 Mb)

Physical page size:     4096 bytes
Minimum physical address:  0x0000000000001000
Maximum physical address:  0x000000001FFEF000




Address space size:     536805376 bytes ( 524224 Kb)

--> Are you sure you want to continue? [y/n] y

Acquisition started at:   [25/4/2011 (DD/MM/YYYY) 19:50:41 (UTC)]

Processing....Done.

Acquisition finished at: [2011-04-25 (YYYY-MM-DD) 19:50:56 (UTC)]
Time elapsed:       0:15 minutes:seconds (15 secs)

Created file size:     536805376 bytes (  511 Mb)

NtStatus (troubleshooting):  0x00000000
Total of written pages:    130957
Total of inacessible pages:     0
Total of accessible pages:   130957

Physical memory in use:     42%
Physical memory size:    523760 Kb (  511 Mb)
Physical memory available:  299656 Kb (  292 Mb)

Paging file size:      788528 Kb (  770 Mb)
Paging file available:    604168 Kb (  590 Mb)

Virtual memory size:    2097024 Kb (  2047 Mb)
Virtual memory available:  2083452 Kb (  2034 Mb)

Extented memory available:    0 Kb (   0 Mb)

Physical page size:     4096 bytes
Minimum physical address:  0x0000000000001000
Maximum physical address:  0x000000001FFEF000

  Address space size:     536805376 bytes ( 524224 Kb)
```

РУКОВОДСТВО ПО СОЗДАНИЮ КРИМИНАЛИСТИЧЕСКИХ ОБРАЗОВ С ПОМОЩЬЮ RIP LINUX

1. Образ операционной системы RIP Linux формата ISO 9660 следует записать на компакт-диск. Убедиться в возможности загрузки операционной системы на компакт-диске до реагирования на инцидент.

2. Подключить к ЭВМ сменный носитель информации, на котором будет создан образ. В качестве такого носителя информации можно использовать внешний НЖМД, подключаемый к ЭВМ по интерфейсу USB. Подключаемый сменный носитель информации следует предварительно отформатировать в файловую систему NTFS.

3. Установить компакт-диск с операционной системой RIP Linux в оптический привод ЭВМ, начать загрузку операционной системы на компакт-диске.

Для загрузки операционной системы на компакт-диске при включении ЭВМ следует обеспечить приоритет оптического привода в списке загрузочных устройств либо непосредственно выбрать оптический привод в качестве загрузочного устройства. Как правило, для изменения списка загрузочных устройств в базовой системе ввода и вывода на раннем этапе загрузки ЭВМ следует нажать клавишу «Delete», а для вывода меню выбора загрузочного устройства — клавишу «F8» или «F9» (более подробные сведения можно найти в документации к ЭВМ или ее компонентам; также в процессе включения ЭВМ на экран будут выведены допустимые сочетания клавиш для базовой системы ввода и вывода, которые необходимы для изменения списка загрузочных устройств или непосредственного выбора загрузочного устройства).

4. В меню загрузчика операционной системы, представленном на рисунке ниже, выбрать подпункт «- Boot Linux system! (skip keymap prompt)» пункта «Boot Linux system! (32-bit kernel)» и нажать клавишу «Enter» (*рис. 1*).

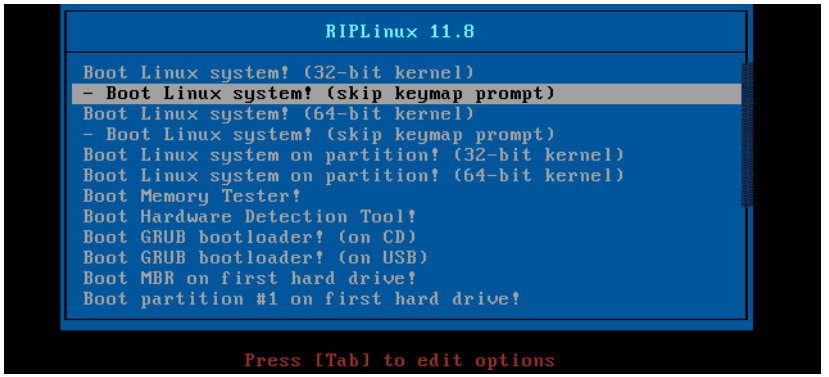

Рисунок 1. *Меню загрузчика операционной системы RIP Linux*

5. После успешной загрузки операционной системы RIP Linux будет отображен запрос ввода имени учетной записи пользователя, представленный ниже. Следует ввести имя учетной записи «root» (без кавычек) и нажать клавишу «Enter». Пароль для данной учетной записи отсутствует (рис. 2).

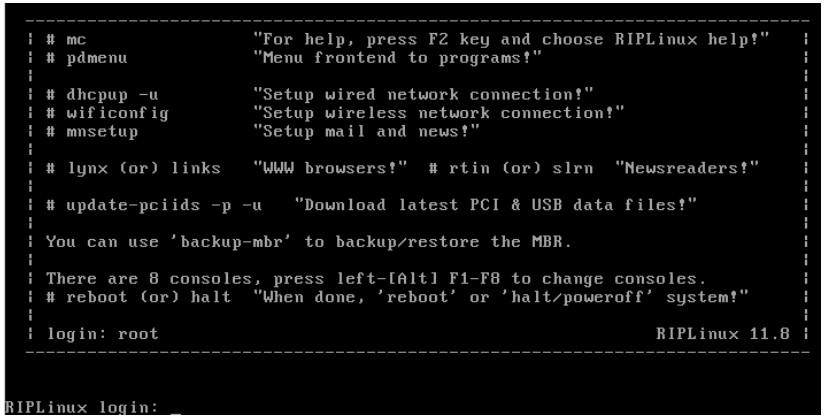

Рисунок 2. *Запрос ввода имени учетной записи*

НА ДАННОМ ЭТАПЕ ОПЕРАЦИОННАЯ СИСТЕМА RIP LINUX ЗАПИСАНА В ОПЕРАТИВНУЮ ПАМЯТЬ ЭВМ И КОМПАКТ-ДИСК МОЖНО ИЗВЛЕЧЬ.

6. Для идентификации адреса носителя информации, подключенного при выполнении пункта 2, ввести команду «parted -l» и нажать клавишу «Enter». В результате будут отображены все зарегистрированные в системе носители информации и их разделы (пример вывода команды представлен ниже).

Идентифицировать адрес подключенного при выполнении пункта 2 носителя информации можно по емкости, отображаемой в выводе команды «parted -l» (*Рис. 3*). Также целесообразно сравнить серийный номер на подключенном внешнем НЖМД с серийным номером, определяемым программно с помощью команды «smartctl -i <адрес устройства>» (где: <адрес устройства> — отображаемый в выводе команды «parted -l» адрес интересующего устройства, например: /dev/hda, /dev/hdb, /dev/sda, /dev/sdb и т. д.). При совпадении серийных номеров следует перейти к выполнению следующего пункта (*рис. 4*). Вывод команды «smartctl -i /dev/hdb» (см. поле «Serial Number»).

7. Создать директорию для монтирования файловой системы носителя информации, подключенного при выполнении пункта 2, следующей командой: «mkdir /mnt/external».

8. Смонтировать файловую систему носителя информации, подключенного при выполнении пункта 2, следующей командой: «mount -t ntfs-3g -o rw <адрес устройства> /mnt/external» (где: <адрес устройства> — определенный при выполнении пункта 6 адрес носителя информации с указанием требуемого номера раздела).

При монтировании файловой системы в первом разделе устройства «/dev/hdb» (*рис. 3*) команда будет выглядеть следующим образом: «mount -t ntfs-3g -o rw /dev/hdb1 /mnt/external».

9. Создать криминалистические образы носителей информации следующей командой:

- dc3dd if=<адрес устройства> of=/mnt/external/<имя файла-образа>

Где: <адрес устройства> — адрес носителя информации, содержимое которого следует скопировать; <имя файла-образа> — имя файла, в который будет скопировано содержимое указанного носителя информации (рекомендуется задавать имена файлов, позволяющие идентифицировать образ, например: «buh-pc-ivanova.dd»).

Пример команды для копирования содержимого носителя информации с адресом «/dev/hda» (вывод этой команды представлен на *рис. 5*):

- dc3dd if=/dev/hda of=/mnt/external/buh-pc-ivanova.dd


```
# parted -l
Model: VBOX HARDDISK (ide)
Disk /dev/hda: 10.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type     File system  Flags
 1      32.3kB  10.7GB  10.7GB  primary  ntfs         boot


Model: VBOX HARDDISK (ide)
Disk /dev/hdb: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type     File system  Flags
 1      32.3kB  21.5GB  21.5GB  primary  ntfs
```

Рисунок 3. *Вывод команды «parted -l»*

```
# smartctl -i /dev/hdb
smartctl 5.41 (build date Mar  8 2011) [i686-pc-linux-gnu-2.6.38.2] (local build
)
Copyright (C) 2002-11 by Bruce Allen, http://smartmontools.sourceforge.net

=== START OF INFORMATION SECTION ===
Device Model:     VBOX HARDDISK
Serial Number:    VBf4843a37-231d2c10
Firmware Version: 1.0
User Capacity:    21,474,836,480 bytes
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   6
ATA Standard is:  ATA/ATAPI-6 published, ANSI INCITS 361-2002
Local Time is:    Tue Apr 26 22:32:20 2011 UTC
SMART support is: Unavailable - device lacks SMART capability.

#
```

Рисунок 4. *Вывод команды «smartctl -i /dev/hdb» (см. поле «Serial Number»)*

```
# dc3dd if=/dev/hda of=/mnt/external/buh-pc-ivanova.dd

dc3dd 7.0.0 started at 2011-04-26 22:55:23 +0000
compiled options:
command line: dc3dd if=/dev/hda of=/mnt/external/buh-pc-ivanova.dd
device size: 20971520 sectors (probed)
sector size: 512 bytes (probed)
145293312 bytes (139 M) copied ( 1%), 6.43605 s, 22 M/s
```

Рисунок 5. *Процесс копирования данных программой dc3dd*

ПРИМЕЧАНИЕ: ПРОГРАММА DC3DD АВТОМАТИЧЕСКИ ПРОПУСКАЕТ НЕЧИТАЕМЫЕ СЕКТОРЫ НОСИТЕЛЯ ИНФОРМАЦИИ, В ОБРАЗ ПО СООТВЕТСТВУЮЩИМ СМЕЩЕНИЯМ ЗАПИСЫВАЮТСЯ НУЛЕВЫЕ БАЙТЫ.

10. После завершения процесса копирования будет выведено соответствующее сообщение (*рис. 6*). Вывод программы dc3dd после завершения копирования данных.

11. Отмонтировать файловую систему сменного носителя информации командой «umount /mnt/external». Отключить сменный носитель информации от ЭВМ.

12. Выключить ЭВМ командой «poweroff».

```
# dc3dd if=/dev/hda of=/mnt/external/buh-pc-ivanova.dd

dc3dd 7.0.0 started at 2011-04-26 22:55:23 +0000
compiled options:
command line: dc3dd if=/dev/hda of=/mnt/external/buh-pc-ivanova.dd
device size: 20971520 sectors (probed)
sector size: 512 bytes (probed)
10737418240 bytes (10 G) copied (100%), 718.31 s, 14 M/s

input results for device `/dev/hda':
   20971520 sectors in
   0 bad sectors replaced by zeros

output results for file `/mnt/external/buh-pc-ivanova.dd':
   20971520 sectors out

dc3dd completed at 2011-04-26 23:07:22 +0000

#
```

Рисунок 6. *Вывод программы dc3dd после завершения копирования данных*

ОБ АВТОРАХ

Максим Суханов
Специалист отдела расследований инцидентов информационной безопасности компании Group-IB. Обладает обширным опытом в области реагирования на инциденты в системах ДБО и проведения соответствующих криминалистических исследований компьютерной информации. Участник международных и отечественных проектов, посвященных судебным компьютерным экспертизам («Компьютерно-техническая экспертиза», «ForensicsWiki» и др.).

Сергей Грудинов
Заместитель гендиректора компании Group-IB. Майор милиции в отставке. С 2010 года работает в Group-IB, до этого времени возглавлял отдел экономической безопасности авиакомпании «Трансаэро». Автор серии семинаров по вопросам юридического и правового сопровождения расследований инцидентов ИБ. Член комиссии по правовым вопросам и комиссии по информационной безопасности и киберпреступности Российской ассоциации электронных коммуникаций.

Алексей Лукацкий
Бизнес-консультант по информационной безопасности компании Cisco. Входит в рабочую группу ЦБ по разработке требований по безопасности Национальной платежной системы (382-П). Участвует в экспертизе нормативно-правовых актов в области информационной безопасности и персональных данных. Является участником подкомитета №1 «Защита информации в кредитно-финансовой сфере» Технического комитета № 122 «Стандартизация финансовых услуг» Федерального агентства по техническому регулированию и метрологии. Является участником подкомитета №127 «Методы и средства обеспечения безопасности ИТ» Технического комитета 22 «Информационные технологии» Федерального агентства по техническому регулированию и метрологии (выполняет функции ISO/IEC JTC 1/SC 27 в России).

Мажоров переулок, д. 14, стр. 2,
г. Москва, Россия, 107023
(495) 661 55 38
info@group-ib.ru
www.group-ib.ru