

## ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКОГО РАССЛЕДОВАНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ПРЕСТУПЛЕНИЙ

В.В. МАЛИКОВ<sup>1</sup>, И.В. БЕНЕДИКТОВИЧ<sup>2</sup>, С.А. ЧУРЮКАНОВ<sup>2</sup>

*Центр повышения квалификации руководящих работников и специалистов  
Департамента охраны МВД Республики Беларусь  
п. Горани, Минский район, 223030, Беларусь*

*Белорусский государственный университет информатики и радиоэлектроники  
П. Бровки, 6, Минск, 220013, Беларусь*

Поступила в редакцию 9 сентября 2013

Предложены технологии обеспечения криминалистического расследования компьютерно-технических преступлений, включающие нормативно-правовые, организационно-технические, технические аспекты раскрытия, расследования и предупреждения таких преступлений.

### Введение

В настоящее время активно развиваются каналы сопряжения и коммуникаций, посредством которых осуществляется on-line доступ к ресурсам мировой сети Internet. Возможности быстрой коммуникации используются гражданами для реализации личных интересов, а также организациями различных форм собственности при осуществлении финансово-экономической деятельности.

Целенаправленное использование высоких технологий со стороны специалистов криминальной сферы деятельности приводит к значительному росту совершаемых компьютерно-технических преступлений (рис. 1).

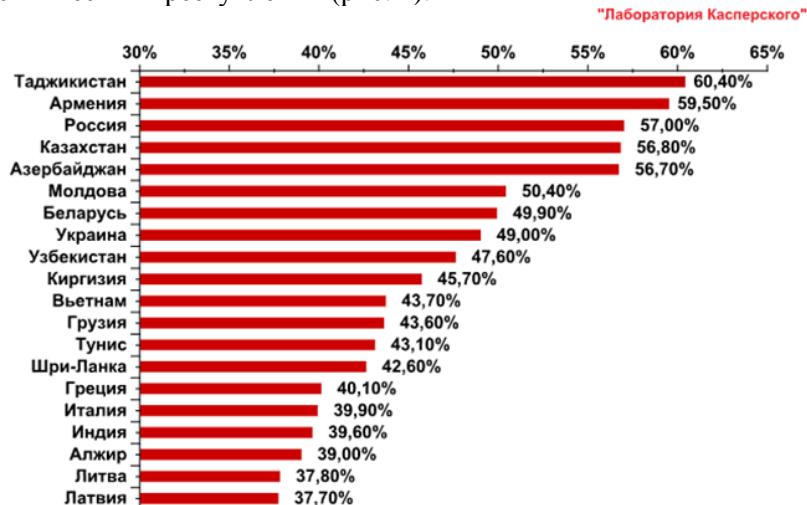


Рис.1. Страны с наибольшим риском заражения компьютеров в сети Internet (1 квартал 2013 г.)

Таким образом существует острые потребность в разработке новых и совершенствовании существующих подходов в нормативно-правовом, организационно-техническом, техническом обеспечении раскрытия, расследования и предупреждения таких преступлений [1].

## **Результаты и обсуждение**

Для описания технологии обеспечения криминалистического расследования следует дать определение следующим понятиям.

Компьютерно-технические преступления – предусмотренные нормативно-правовыми актами действия, в которых компьютерно-техническая информация является объектом преступного посягательства [2].

Компьютерно-техническая информация – сведения (сообщения, данные, технологический/аппаратный код, оптические/электромагнитные параметры среды обработки), представленные в электронно-цифровой форме, зафиксированные на материальном носителе, обрабатываемые аппаратно-программными устройствами, а также передающиеся по каналам сопряжения и коммуникации посредством электромагнитных сигналов.

Основным объектом исследования при проведении криминалистического расследования компьютерно-технического преступления является криминальный электронно-цифровой след – криминалистически значимая компьютерно-техническая информация (сообщения, данные, технологический/аппаратный код, оптические/электромагнитные параметры среды обработки), имеющая следующие характеристики.

1. Является неотъемлемой частью итогового электронно-цифрового следа, возникающего в ходе обработки оригинальной компьютерно-технической информации;

2. Вносит дополнительные обратимые/необратимые изменения в оригинальные сообщения, данные, технологический/аппаратный код, оптические/электромагнитные параметры среды обработки, в итоге нарушающие свойства их целостности, доступности и конфиденциальности;

3. По способу документирования подразделяется на энергозависимую и энергонезависимую.

Основную роль в подготовке и реализации компьютерно-технических преступлений играет криминальный организатор [3].

Криминальный организатор – физическое лицо/группа лиц, юридическое лицо/группа лиц, незаконные организации/группировки, государство/группа государств осуществляющих полное или частичное: планирование и/или разработку, внедрение механизмов, приводящих к осуществлению компьютерно-технического преступления (рис. 2).

В настоящее время можно выделить следующие основные типы криминальных организаторов: спецслужбы иностранных государств и блоков государств, террористы и террористические организации, конкурирующие организации и структуры, криминальные структуры, взломщики программных продуктов, недобросовестные сотрудники и партнеры, бывшие сотрудники организаций, пользователи услугами (сервисами).

В качестве мотивов криминального организатора следует отметить: месть, достижение денежной выгоды, хулиганство/любопытство, профессиональное самоуверждение, политическая/идеологическая выгода [4].

Криминальный организатор компьютерно-технического преступления может осуществлять полный цикл планирования и/или разработку, внедрение механизмов как самостоятельно, так и с привлечением сторонних средств и сервисов, приобретаемых на возмездной основе. Условный механизм приобретения таких средств, систем и услуг показан на рис. 3.

Основной задачей криминального организатора компьютерно-технических преступлений, связанной с завершением реализации механизмов хищения финансово-регистрационных данных, является вывод финансовых средств через подставные юридические и/или физические лица. Один из таких криминальных механизмов с использованием подставных физических («дропов») и юридических лиц показан на рис. 4. Наибольший интерес для криминального организатора компьютерно-технических преступлений представляют безналичные электронные платежи пользователей сервисов сети Internet.

Экспloit-пак – сборка компьютерных программ, фрагментов программного кода или последовательность команд, использующих уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерно-техническую систему. Наиболее известные базы знаний по уязвимостям и сборники экспloit-паков: ICS-CERT, NVD, CVE,

Bugtraq, OSVDB, Mitre Oval Repositories, exploit-db, Siemens Product CERT, SAINTExploit, Metasploit Framework, Immunity Canvas, Agora Pack, Agora SCADA+, D2 Exploit Pack, White Phosphorus exploit pack, VulnDisco Exploit Pack, BlackHole, Sakura.

Абзуостойчивый хостинг (bulletproof hosting service) – это хостинг, размещенный в странах которые не имеют законодательных рычагов влияния на владельцев сервисов/серверов с не законной информацией, с предоставлением гарантии минимального риска его блокировки.

Криминальный арбитраж – криминальные структуры, осуществляющие незаконные услуги по обеспечению имущественных и не имущественных прав/гарантий между криминальным организатором и разработчиками на бирже криминальных средств, систем и услуг, а также взыскания/возмещения ущерба понесенного сторонами в ходе нарушения условий криминальной сделки.



Рис. 2. Схема организации компьютерно-технического преступления

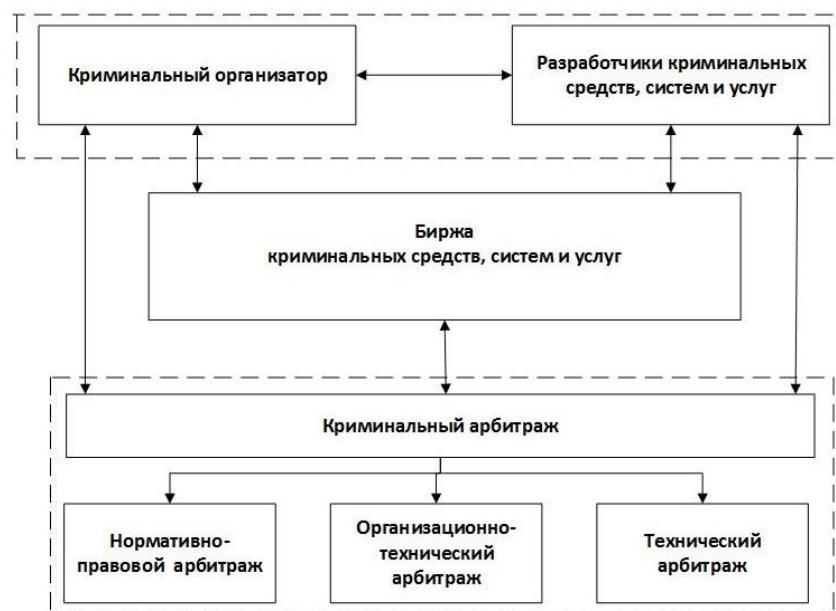


Рис. 3. Схема организации функционирования биржи криминальных средств, систем и услуг

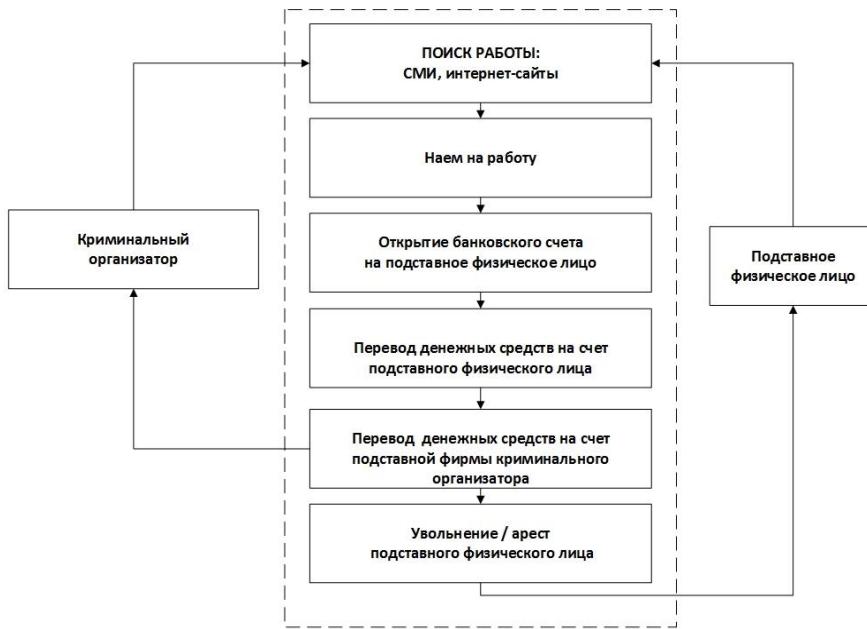


Рис. 4. Схема вывода финансовых средств через подставные физические и/или юридические лица

Атаки на сервисы безналичных электронных платежей возможна как на сторону серверной инфраструктуры владельца сервиса, так и на компьютер конечного пользователя. Учитывая то, что как правило серверная инфраструктура защищена более надежно, на практике быстрее и экономически целесообразнее осуществить компьютерно-технический взлом компьютера конечного пользователя. Масштабируя эффект взлома на тысячи пользователей таких сервисов криминальный организатор достигает крупного финансово-экономического результата [5]. Основные варианты перехвата управления в сервисах безналичных электронных платежей приведены на рис. 5.



Рис. 5. Схема перехвата управления в сервисах безналичных электронных платежей

Для устранения возможностей перехвата и повышения уровня безопасности платежными сервисами используется алгоритм двухфакторной аутентификации пользователя. Однако, наиболее развитые и технологичные троянские программы, используемые киберпреступниками, например банковский троянец Zeus (Zbot) совместно с мобильным троянцем Zeus-in-the-Mobile (ZitMo), могут обходить данную систему защиты (см. рис. 6).

Другие системы защиты сервисы безналичных электронных платежей также нейтрализованы киберпреступниками:

- система chipTAN – банковский троянец SpyEye;
- система на основе USB-токена – банковский троянец Lurk.



Рис. 6. Схема обхода двухфакторной аутентификации в сервисах безналичных электронных платежей

Механизм заражения компьютера пользователя сервиса безналичных электронных платежей вредоносным программным обеспечением (ПО), основанный на эксплойт-паках (Nuclear Pack, Styx Pack, BlackHole, Sakura) реализующих уязвимости в легитимном ПО, изображен на рис. 7.

Например, в марте 2013 г. эксплойт-пак BlackHole использовал эксплойты к следующим уязвимостям:

- версия Java от 1.7 до 1.7.x.8 – CVE-2012-5076;
- версия Java меньше 1.6 или от 1.6 до 1.6.x.32 – CVE-2012-0507;
- версия Java от 1.7.x.8 до 1.7.x.10 – CVE-2013-0422;
- версия Adobe Reader меньше 8 – CVE-2008-2992;
- версия Adobe Reader равна 8 или от 9 до 9.3 – CVE-2010-0188;
- версия Adobe Flash от 10 до 10.2.158 – CVE-2011-0559;
- версия Adobe Flash от 10.3.181.0 до 10.3.181.23 и меньше 10.3.181 – CVE-2011-2110.



Рис. 7. Схема заражения компьютера на основе эксплойт-паков ПО

Организовано экспериментальное обследование сайтов более 30 банков Республики Беларусь на предмет уязвимостей, описанных в базах знаний по уязвимостям и сборниках эксплойт-паков [6]. Получены следующие результаты.

1. Сканер Sucuri SiteCheck: 1 сайт – имел критическую уязвимость кода, 2 сайта – инсталлированные системы интернет-статистики с внешним обменом данными, 2 сайта – работают на web-серверах с повышенным риском ошибок администрирования и взлома.

2. Рейтинг безопасности Norton Safe Web – 6 сайтов не имеют рейтинга.

3. Рейтинг безопасности McAfee SiteAdvisor – 9 сайтов не имеют рейтинга.

Таким образом, более 60 % исследованных сайтов имеют потенциальные уязвимости, которые могут быть использованы для осуществления компьютерно-технических преступлений.

### **Заключение**

Предложенные технологии обеспечения криминалистического расследования компьютерно-технических преступлений, включающие нормативно-правовые, организационно-технические, технические аспекты раскрытия, расследования и предупреждения таких преступлений, позволяют повысить эффективность работы специалистов отрасли информационной безопасности. Выявленные уязвимости сайтов банков Республики Беларусь были доведены до соответствующих служб безопасности.

## **TECHNOLOGIES FOR PROVIDING OF FORENSIC INVESTIGATION OF COMPUTER AND TECHNOLOGY CRIMES**

V.V. MALIKOV, I.V. BENEDIKTOVICH, S.A. CHURUKANOV

### **Abstract**

Technologies for providing of forensic investigation of computer and technical crimes involving legal, organizational and technical components which provide detection, investigation and prevention of such crimes are proposed.

### **Список литературы**

1. *Лепехин А.Н.* Расследование преступлений против информационной безопасности: теоретико-правовые и прикладные аспекты: монография. Минск, 2008.
2. *Вехов В.Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки: Автореф. ... докт. юрид. наук: Волгоград, 2008.
3. Расследование компьютерных преступлений: услуги и решения // group-ib.ru. [Электронный ресурс]. – Режим доступа: [http://www.group-ib.ru/images/media/Group-IB\\_Catalogue\\_int.pdf](http://www.group-ib.ru/images/media/Group-IB_Catalogue_int.pdf) – Дата доступа: 20.09.2013.
4. *Стефаров А.П.* Разработка типовой модели нарушителя правил разграничения доступа в автоматизированных системах: Автореф. ... дис. канд. техн. наук. Красноярск, 2013.
5. Защита от виртуальных грабителей // securelist.com. [Электронный ресурс]. – Режим доступа: <http://www.securelist.com/ru/analysis/208050811/> Zashchita\_ot\_virtualnykh\_grabiteley – Дата доступа: 21.09.2013.
6. *Маликов В.В.* // Электроника инфо. 2013. № 6 (96). С. 16–18.