tion and communication technologies. The average and budget according to the world practice which have to be set aside for the system of information security is between 10-20 % from the value of the information system. Even when the information security level in the organization is on low and unenviable level, it's very hard and specific for the information security specialists to present the need of financing this system and the best approach for that is the presentation to be from the aspect of economy logic and with economically based arguments.

Because of the resource reduce, the resources that the organization invest in the information security , and one of the most important modes which will contribute for successful functioning of the systems for information security is optimization of the same, so they will be effective and efficient and would have economic justification.

Иван Бабенко,
Кишинэу, Молдова

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ INTERNET

This article will provide a general overview for Internet-crimes investigation on evolution trends, and on related Forensic. Also, you can find examples of such crimes and general investigative methods.

Преступления в сфере информационных технологий увеличивают своё количество и, как следствие, опасность для населения. Это происходит за счёт всё большей информатизации, распространения беспроводных технологий и использования ресурсов сети Internet. По исследованиям компании Gartner в 2008 году объём злоумышленного трафика по сравнению с 2006 увеличился более чем в 2 раза. По статистике ФБР (FBI) доля преступлений, совершённых в 2008 году, с использованием сети Internet по отношению к общему числу компьютерных преступлений составила около 55%. По тем же данным основная группа жертв таких преступлений – это люди в возрасте 30-49 лет (около 50%). На долю же остальных возрастных групп выпадает почти равномерное распределение риска (относительно их количества) стать жертвой компьютерного преступления. В десятку самых опасных стран по количеству компьютерных злоумышленников были признаны США (60,9%), Великобритания (15,9%), Нигерия (5,9%), Канада (5,6%), Румыния (1,6%), Италия (1,2%), Нидерланды (1,2%), Россия (1,1%), Германия (0,7%) и ЮАР (0,6%).

За прошедший 2008 год было совершено более 14000 правонарушений в пространстве русскоязычного Интернета по сведениям МВД РФ, при этом было заведено 5 572 уголовных дела. В Молдове, несмотря на более развитое законодательство, пока нет таких грандиозных успехов в области обнаружения и раскрытия компьютерных преступлений. В условиях финансового кризиса киберпреступность показывает и будет показывать стремительный прирост, поэтому, необходимо активно работать над предупреждением таких преступлений, а также над их расследованием.

Особенное внимание необходимо уделить расследованию Internet-преступлений, так как из-за относительной простоты и доступности совершения такого преступления возникает специфическая проблема восприятия этих преступлений. Отмечу особенности и отличительные черты Internet-преступлений:

Преступления совершаются не только с корыстными или иными преступными целями, но и случайно из любопытства или незнания того, что действия являются незаконными. Они имеют следующие особенности:

1. Очень часто такие преступления носят международный характер;
2. Трудно предугадать или предотвратить замышляемое преступление;
3. Не всегда закон настолько развит, чтобы дать следователю возможность получить все необходимые ему данные;
4. Очень сложно доказать причастность следов к преступлению;
5. Судебная система не всегда подготовлена для понимания экспертизы, а также для понимания состава преступления.

В ходе расследования любого преступления необходимо изначально понимать, с каким именно типом преступления приходится иметь дело и, основываясь на некоторых общих методах, строить следственную работу.

Типы преступников, существующих в сети Internet, условно можно разделить на 3 категории: *любопытные или шутники, разрушители или вандалы и целенаправленные взломщики*.

Эти злоумышленники могут, используя Internet, совершать такие преступления, как: *On-line мошенничество, клевета, оскорбления и экстремистские действия, DOS-атаки, Deface, запуск вредоносных программ, мошенничество с трафиком, нарушение авторских прав, фишинг, кибersквоттинг, мошенничество с электронными платежами, терроризм, Real-time black-lists, кардинг и др.*

Эти преступления могут быть различных масштабов: *международные, национальные, корпоративны, против личности*.

В любом случае классы преступлений не стоит рассматривать, как законченный список и, рекомендации по каждому классу тоже не должны восприниматься догматично, так как в любой ситуации работа следователя должна строиться на его личном опыте и методике с привязкой к конкретной ситуации. Хотя

утверждать о каких-либо стандартных схемах расследования Internet-преступления сложно, обычно оперативно розыскные мероприятия (ОРМ) включают в себя следующее:

- Исследование и перехват трафика по установленным каналам связи;
- Установление принадлежности IP-адреса или домена злоумышленника – *локация провайдера соответствующей услуги и выяснение у него информации о принадлежащем ему IP-адресу и статистике по его трафику. Обычно этот этап сопряжён со сложностями конфиденциальности информации о клиентах, поэтому провайдеры стараются ограничиться самостоятельным предупреждением клиента или разрывом контракта с ним без вмешательства правоохранительных органов*;
- Установление принадлежности иных средств, вовлечённых в преступление, – *почтового адреса, стороннего сервера, файла, программ, фотографий, портативных носителей и др.*;
- Поиск следов на сервере и системе (месте преступления): *анализ логов, жестких дисков, кэша, переписки, исходных текстов программ, нелицензионных продуктов и иных следов преступных действий*;
- Поисковые машины в качестве методики ОРМ. *После сбора информации можно прибегнуть к помощи поисковых машин для установления личности преступника, нахождения дополнительной информации и преступнике, выявления фиктивных аккаунтов, нахождения большего количества пострадавших от преступления*;
- Социальная инженерия, как метод ОРМ, *представляет собой также достаточно хороший способ выявления преступника и получения информации о нём от его знакомых, близких, заказчиков, партнёров и других лиц, обладающих информацией. Также при помощи таких методов можно организовать очень простую слежку за средствами связи злоумышленника и спровоцировать злоумышленника на рецидив.*

Расследование компьютерных преступлений сопряжено с проблемой выявления доказательной базы для выдвижения обвинений. Это обычно сопряжено с некоторыми трудностями, как технологического характера и отсутствия чётких стандартов в области экспертизы, так и с проблемами запутывания следов и сокрытия информации, которые в информационной среде становятся ещё более неуловимыми в процессе следственного процесса.

На рисунке 1 показана цепь событий в расследовании компьютерного преступления.

Кроме того, преступники используют изощрённые методики для сокрытия доказательств своих действий. Среди этих методов – *шифрование и пароли, компрессия файлов,*

стеганография, отдаленное хранение, анонимные средства связи, использование открытых источников, компьютерное проникновение, «зомбирование компьютеров», «групповой взлом» и др.

Поэтому иногда очень сложно выявить доказательства компьютерного преступника, а при их комбинированном использовании – сбор доказательной базы может использовать много ресурсов или вовсе не дать никаких результатов. Даже при наличии спец. средств и технологий сбора доказательств и КТЭ (компьютерно-технической экспертизы) их количество и качество для работы на государственном уровне оставляет желать лучшего, так как не все из существующих средств обладают необходимой сертификацией для того, чтобы собранную ими информацию можно было представлять в виде доказательства в суде. Для недопущения совершения таких преступлений *в коммерческих структурах* необходимо внедрение политики безопасности и периодический внутренний и сторонний аудит. *На уровне государства* это должно решаться посредством принятия национальных законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы по борьбе с киберпреступностью и международные стандарты в области ИБ, такие как: ITIL, COBIT, ISO 27001.

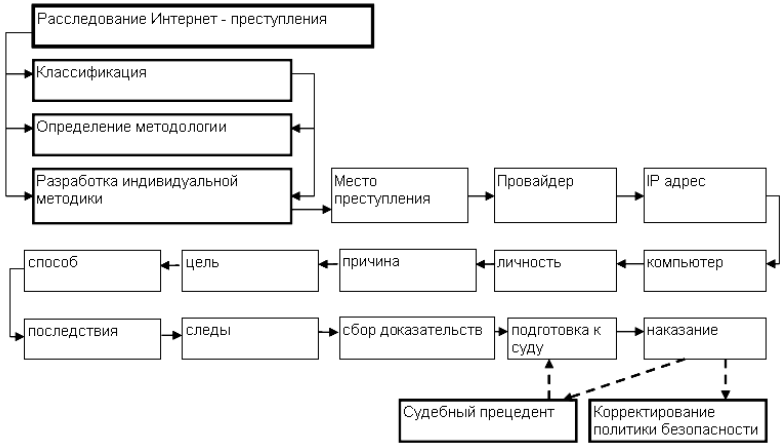

***Рис. 1.* Последовательность расследования киберпреступления**

Необходимо учитывать появление новых видов преступлений в среде Internet, которые либо сложно классифицировать, либо вообще невозможно определить как преступление. Рассмотрим несколько таких преступлений:

Обнаруженная «дыра» в одной из микроблоггинговых социальных сетей позволила злоумышленникам получить доступ к аккаунту нынешнего президента США Барака Обамы. До устранения всех

последствий взлома этот аккаунт был отредактирован злоумышленником. Признать этот факт актом кибертерроризма в теории можно, но в практике доказать достаточно сложно. Большинство таких преступлений проходят по другим статьям, хотя людей, их спровоцировавших, достаточно сурово наказывают людей их спровоцировавших. Тем не менее, кибертерроризм в Internet существует.

Или другой пример. Приватные данные о личности хотя и по согласию пользователя, но без всякой альтернативы предоставлены в общий доступ в некоторых социальных сетях. При этом владельцы некоторых сервисов за закрытие учётных записей пользователя взимают с пользователей оплату, что, так или иначе, противоречит праву пользователя на защиту личной информации.

Известная программа-клиент для обмена мгновенными сообщениями использует несколько протоколов для отправки сообщений и при первом же запуске требует ввести и сохранить на своём сервере данные об учётных записях пользователя в различных других сервисах. У пользователя буквально «выманивается» его персональная информация. Сейчас такие преступления остаются безнаказанными, так как не противоречат принципиально закону и пока не угрожают обществу, но надзор и противостояние за такими вещами, пусть не в уголовном, но в административном порядке, просто необходим.

Заключение:

Internet является местом, где пользователь чувствует себя максимально анонимно и раскованно. Сеть является открытым международным пространством и преступление, совершённое в одном конце воздушного шара, может иметь отголосок на другом конце планеты. И это происходит в то время, когда национальные органы правопорядка чаще всего не имеют возможности противостоять таким преступлениям. Поэтому необходимо развивать международные службы по борьбе с Internet-преступлениями, контролировать ситуацию с ресурсами национальных сетей, а также перейти к коммерческому регулированию этой проблемы, то есть организовать почву для частного сыска и частной компьютерной экспертизы. Это даст пользователям Internet почувствовать, что сеть – это такой же мир, где нужно соблюдать все законы с одной стороны, а с другой стороны – дать человеку возможность чувствовать себя в сети безопасно. Также необходимо развивать и дополнять специфическую методологию расследования Internet-преступлений для повышения эффективности и согласованности следственной работы, а также для адаптации судебной системы ввиду новых преступлений.