«Борьба с Интернет преступностью»
12-13 июня 2013 года

ИНТЕРНЕТ-ПРЕСТУПНОСТЬ КАК НОВАЯ УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ:МЕЖДУНАРОДНЫЙ АСПЕКТ

Голубев Владимир Александрович
Махно Виталий Владимирович
Компания «Cyber Safety Unit»
Корпорация «NOOSPHERE VENTURES»

Донецкий юридический институт МВД Украины

Каждый гражданин Украины должен знать, как защитить себя в киберпространстве

4 месте в мире

Top 15 der Ursprungsländer von Angriffen des Vormonats

	Quelle des Angriffes	Anzahl der Angriffe
	Russian Federation	2,402,722
	Taiwan, Province of China	907,102
	Germany	780,425
	Ukraine	**566,531**
	Hungary	367,966
	United States	355,341
	Romania	350,948
	Brazil	337,977
	Italy	288,607
	Australia	255,777
	Argentina	185,720
	China	168,146
	Poland	162,235
	Israel	143,943
	Japan	133,908

Украина оказалась на **4** месте в мире по количеству исходящих из страны кибератак. Об этом свидетельствует исследование ведущего немецкого оператора связи Deutsche Telekom, который визуализировал карту стран-источников кибератак.

Источник: http://www.crime-research.ru/news/09.03.2013/7514/

Интернет - преступность

- Распространение компьютерных вирусов
- Хищение денежных средств
- Распространение детской порнографии
- Атаки в сети
- Интернет-мошенничество

Хищение денежных средств

Существует много видов уголовных правонарушений, связанных с использованием компьютеров, в рамках которых имеет место хищение денежных средств:

- атаки хакеров на банки или финансовые системы;
- мошенничества, связанные с переводом “электронных” денег;
- мошенничества с банковскими пластиковыми картами.

Виртуальный криминал

По информации НБУ Украины, за 2012 г. общее количество мошеннических операций с платежными картами в нашей стране выросло сразу на 47% и с 35 до 57 увеличилось количество банков, со счетов которых пропадали средства. Как и прежде, по числу несанкционированных списаний со счетов лидировали физлица (ежедневно от населения поступает до 50 жалоб, со счетов за прошлый год пропало 11,4 млн грн.).

Shiming

На смену скимминга, пришел новый вид кражи денег с банковских карт.

В соответствии с названием с данной технологией «Шим» (**shim** — тонкая прокладка), вместо традиционных громоздких накладок на щель приёмника пластиковых карт банкоматов (скиммеров), в шимминге используется очень тонкая, гибкая плата, внедряющаяся через эту щель внутрь банкомата и практически незаметна.

МВД постоянно выявляет следы мошеннических накладок на банкоматы

По данным министерства, в 2011 году было выявлено 45 таких аппаратов, в 2012 – 73, а за первый квартал 2013 года было выявлено уже 37 устройств.

Количество выявленных в Украине скимминговых устройств в 2012 году возросло на 62%, а в 2013 году следы таких устройств уже выявляются несколько раз в неделю, сообщил заместитель начальника Управления по борьбе с киберпреступностью МВД Украины Леонид Тимченко

Источник: http://interfax.com.ua/

Фишинг - как бороться?

Внешний вид таких страниц обычно идентичен настоящей, однако есть ряд отличительных признаков:

- как правило у фишинговых страниц в правой части адресной строки браузера отсутствует изображение замка, свидетельствующего, что обмен данными происходит по защищенному соединению, адрес в адресной строке начинается не с **https://, а с http://;**

- Как правило на «фишинговой» странице сообщения, мошенники просят ввести полученный от банка **разовый пароль**, **номер мобильного телефона** и т.д.

По данным МВД Украины:

С января по конец ноября 2012 года в Украине возбудили 745 уголовных дел по киберпреступлениям, в этот период было осуждено 113 человек.

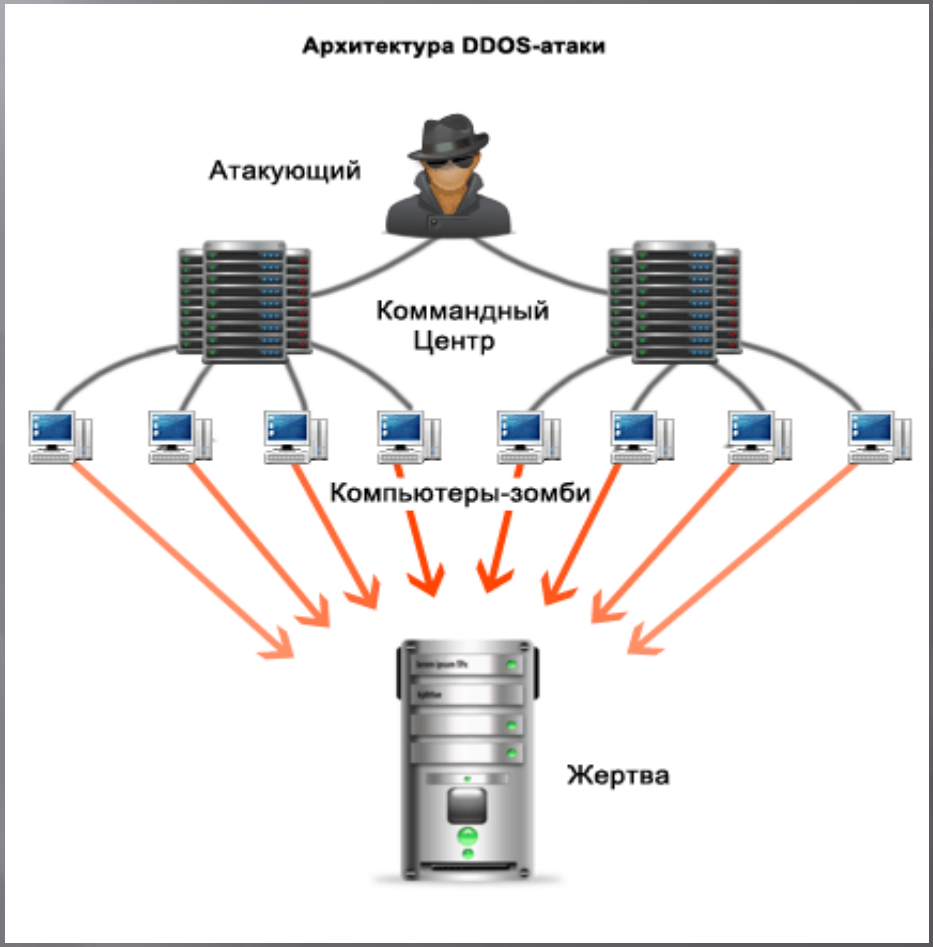
По данным МВД России:

Количество киберпреступлений в России, зарегистрированных правоохранительными органами в 2012 году, выросло почти **на треть** по сравнению с 2011 годом.

По информации начальника Бюро специальных технических мероприятий МВД РФ Алексея Мошкова, в 2012 году в России было зарегистрировано на **28 %** больше высокотехнологичных преступлений по сравнению с 2011 г.

DDoS (Distributed Denial of Service)

Одна из самых распростаненных атак –
атака «отказ в обслуживании»



Цель DDoS атаки – парализовать работу атакуемого узла.

«Хак-услуги»…


Сколько стоят услуги хакеров
Цена
1260 грн.
Разослать спам - 2,2 млн. пользователей. В некоторых фирмах предлагают скидку 26% к 26-летию первого спама в мире
Заказать DDOS-атаку. Цена за сутки, в зависимости от ресурса
Цена
$50–1500
Цена
$20–30
Взломать аккаунт ВКонтакте, или профиль в ICQ
По информации профильных сайтов

Финансовый ущерб

Финансовые и коммерческие потери из-за DDoS (упущенный доход, отток клиентов, снижение производительности труда и ухудшение репутации) намного превышают прямые, операционные убытки.

Защита от DDoS-атак

Защита от DDoS заключается в отсечении паразитного трафика на уровне предприятия и провайдера доступа в интернет, а также в нейтрализации сетей ботнетов, осуществляющих распределённые атаки.

Международный аспект

На сегодняшний день, основным документом, регулирующим вопросы международного сотрудничества в борьбе с киберпреступностью является **«Конвенция о киберпреступности».**

Конвенция устанавливает меры, которые должны предпринять страны на национальном уровне в отношении правонарушений против конфиденциальности, целостности и доступности компьютерных данных и систем, правонарушений, связанных с компьютерами, правонарушений, с распространением детской порнографии и правонарушений, связанных с нарушением авторских и смежных прав.

http://www.alppp.ru/law/pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii---185-rus--angl-.html
(Будапешт, 23 ноября 2001 года)

Европейской конвенции о киберпреступности

Отдельный раздел Конвенции посвящен международному сотрудничеству по вопросам экстрадиции в связи с уголовными правонарушениями, предусмотренными Конвенцией, добровольного предоставления информации относительно проведения расследования уголовных преступлений, определенных Конвенцией, а также процедур, связанных с запросами о взаимной помощи в случае отсутствия международных соглашений между странами.

Европейское сотрудничество

По данным Евросоюза, ежедневно жертвами преступлений, совершаемых в Сети, становится не менее одного миллиона человек. Совокупный ущерб от них достигает 300 миллиардов евро в год.

С киберпреступностью борются все страны Евросоюза, но до сих пор – отдельно друг от друга и с весьма переменным успехом. Многие национальные правоохранительные органы быстро достигают пределов своих возможностей, ведь место преступления в сети Интернет – границ не имеет.

По линии ПАСЕ

11 апреля 2013 г. на заседание Совета Межпарламентской Ассамблеи СНГ, в своем обращении глава ПАСЕ Жан-Клод Миньон (Jean-**Claude** Mignon), предложил развивать сотрудничество по юридическим вопросам, а также в борьбе с киберпреступностью

Европейский центр по борьбе с киберпреступностью

The European Cybercrime Centre - EC3

Для коллективного противодействия угрозам киберпреступности 11 января 2013 г. начал работу Европейский центр по борьбе с киберпреступностью. Он является структурным подразделение Европола (Europol) со штаб-квартирой в Гааге.

Среди приоритетов Центра, расследования Интернет-мошенничества, в частности в системе электронного банкинга и противодействие Интернет-педофилии

Contacts Cybercrime Centre - EC3

Contact

Cornelia Riehle
Deputy Head of Section
European Criminal Law, ERA

Tel. +49 (0)651 937 37 302
Fax +49 (0)651 937 37 773
Email criehle@era.int

Elizabeth Klopocki
Assistant
European Criminal Law, ERA

Tel. +49 (0)651 937 37 322
Fax +49 (0)651 937 37 773
Email eklopocki@era.int

Наша Компания «Cyber Safety Unit», уже установила первые контакты, пока на уровне обмена почтой и обсуждением точек соприкосновения и объединения усилий в противодействии киберпреступности с Европейским центром по борьбе с киберпреступностью.

Директор Европейского центра по борьбе с киберпреступностью Троелс Оертинг (Troels Oerting, Assistant Director, Europol & Head, European Cybercrime Centre)

Сотрудничество в рамках СНГ

Сложность проблем, которые характерны для уголовных правонарушений в сети Интернет, делает необходимым тесное сотрудничество между общественными организациями, экспертами и правоохранительными органами стран СНГ в этой области. В этом направлении, нашей компанией, осуществляется сотрудничество в форме обмена информацией, проведению расследований компьютерных инцидентов и оказания содействия в подготовке кадров сотрудников правоохранительных органов Республики Казахстан, Молдовы и Российской Федерации.

Некоторые выводы

Для эффективной борьбы с киберпреступностью нужна система мер и реализация соответствующей государственной политики в этой области.

Одни лишь новые законы не способны противостоять росту IT-преступности. Нужен комплекс мер, нацеленных не только на развитие правоприменительной базы, но и на повышение уровня грамотности граждан, судебных и правоохранительных органов.

Проект «Cyber Safety Unit»

Одна из наших главных задач– это организация плодотворного взаимодействия с право-охранительными органами в сфере борьбы с киберпреступностью, а также оказание помощи компаниям, пострадавшим от кибератак.

Cyber Safety Unit
Направления деятельности

Международное сотруднечество

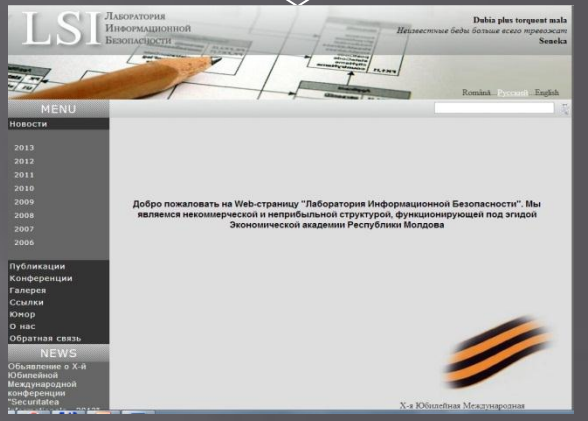
Российская Федерация

http://www.cyberpol.ru/
Интернет-проект посвященный вопросам противодействия киберпреступности

Республика Казахстан

http://kz-cert.kz/ru/
Служба реагирования на компьютерные инциденты (KZ-CERT).

Республика Молдова



http:// Security.ase.md
Лаборатория информационной безопасности Молдавская Экономическая Академия

Международное сотрудничество

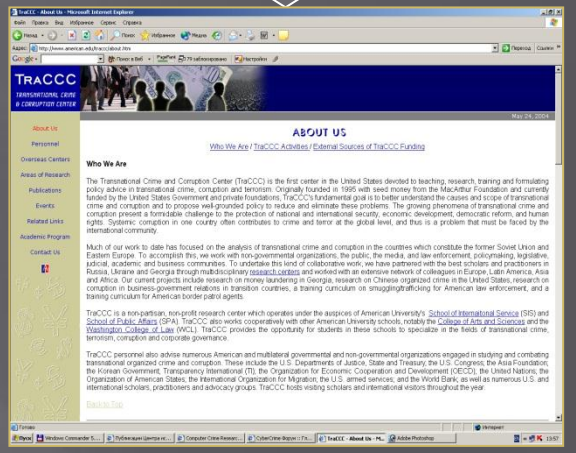
Great Britain

http://www.4law.co.il/nh1.htm
http://www.soca.gov.uk/
NHTCU – the National Hi-Tech Crime Unit
Serious Organised Crime Agency
(Between 2001 and 2006 the UK's National Hi-Tech Crime Unit)

Korea

http://www.kias.or.kr/
Korea Information Assurance Society
Kyonggi University
(Отдел защиты информации Корейского университета)

США



http://policy-traccc.gmu.edu/
Terrorism, Transnational Crime and Corruption Center (TraCCC)
(Центр по изучению транснациональной организованной преступности и коррупции при Американском Университете)

Cyber Safety Unit

Голубев Владимир Александрович
директор Департамента
противодействия киберпреступности
Компании “Cyber Safety Unit”
Корпорации NOOSPHERE VENTURES

Благодарю за внимание!

E-mail: vladimir@crime-research.org
office@kodekschesti.com
Phone: +38(061)2340292
Mobile: +38(050)3225496