УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО
ФАКУЛТЕТ „ПРИЛОЖНА ИНФОРМАТИКА И СТАТИСТИКА“

ПРИЛОЖНА ИНФОРМАТИКА И СТАТИСТИКА - СЪВРЕМЕННИ ПОДХОДИ И МЕТОДИ

Международна научна конференция
25 - 26 септември 2009 г.
Равда, България

УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО "СТОПАНСТВО"

УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО
ФАКУЛТЕТ „ПРИЛОЖНА ИНФОРМАТИКА И СТАТИСТИКА“

ПРИЛОЖНА ИНФОРМАТИКА И СТАТИСТИКА - СЪВРЕМЕННИ ПОДХОДИ И МЕТОДИ

Международна научна конференция
25 - 26 септември 2009 г.
Равда, България

УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО "СТОПАНСТВО"
София, 2010

© УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО "СТОПАНСТВО"

Директор: доц. д-р Милчо Толев, тел. 81-95-564
Гл. редактор: Ваня Миленкова, тел. 862-88-57, 81-95-359
Худ.-техн. редакция: Истилиян Божилов, тел. 81-95-517
Счетоводство: Румяна Машкова, тел. 81-95-665

УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО
София, Студентски град "Христо Ботев"

СЪДЪРЖАНИЕ

СЕНЧЕСТИЯТ ПАЗАР НА ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

доц. д-р Агоп С. Саркисян,
Стопанска академия "Д. А. Ценов",
проф. д.ик.н. Сергей А. Охрименко,
Лаборатория по информационна сигурност,
Молдовска икономическа академия,
Кишинев, Молдова

Схващам света, за да бъде чут през третото хилядолетие - единствено като поле за културно състезание между народите
Гоце Делчев, 1903 г.

ВЪВЕДЕНИЕ

Развитието на информационните и комуникационните технологии промени коренно нашето ежедневие, управлението на икономическите и социалните процеси, превърна се в доминиращ фактор на устойчивото развитие на обществото. В настоящия момент средствата за информатизация заемат голяма част от световния пазар и определят в значителна степен структурата на инвестиционните потоци. Необходимо е да виждаме не само положителните промени, но и възможната опасност и рисковете, които, ако не се вземат под внимание и се подценяват, могат да доведат до сериозни последици. Пазарът на информационни технологии по своя обем изпревари пазара на природни ресурси. Но едновременно с това загубите, свързани с правонарушенията при събиране, обработване и разпространяване на информационните продукти и услуги, възлизат на астрономически цифри. Информационните технологии навлизат все по-дълбоко в нашето ежедневие, а заедно с тях - и киберпрестъпността. Неразбирането на сериозността на този проблем съвсем не означава, че той не съществува. Негативното въздействие на сенчестите информационни технологии обективно е налице и се засилва, и е необходимо да се подготвим за него. Тази изходна предпоставка формира основата на настоящата статия.

СЕНЧЕСТИ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Не е тайна, че паралелно с официалния многомилиарден пазар на информационни и комуникационни технологии съществува и "сенчест" пазар на продукти и услуги. Структурата на този "сенчест" пазар е доста разнообразна и включва множество сегменти. На първо място това се отнася за дейността, която е свързана с такива категории като "фишинг", "спам", "хакинг", "кракинг", "кардинг", "присвояване на система", "спуфинг", "сенчести изчисления", "инсайдер", "офшорен кибертероризъм" и много други. Наблюдава се създаване на специализирани групи "по интереси". Към тях спадат групи, които се специализират в следните направления на дейността:

- написване на зловреден код с цел извършване на различни действия за несанкциониран достъп до информационните ресурси на потребителите и информационните системи;
- разпращане на спам;
- организиране на отдалечени и разпределени атаки срещу информационните системи (DoS и DDoS);
- създаване на ботнети като "стартова" площадка и даването им под наем с цел реализиране на комплекс от противоправни действия;
- кражба на идентификационните данни на ползващите кредитни карти и изготвяне на фалшиви кредитни карти;
- премахване на защитните средства от лицензирания софтуер;
- търговия с нелицензиран софтуер;

- търговия с несъществуващи продукти и услуги, "мошеничеството като услуга" (по аналогия със "софтуера като услуга") и много др.

Посочените групи и тяхната противоправна дейност се характеризират с едно съдържателно определение - киберпрестъпност. Главната цел на настоящата статия е разглеждане на криминалната дейност по създаването на ботнети като най-опасна от гледна точка на възможните последици, а също така на потенциалните икономически загуби от тяхната дейност. Като основна предпоставка за противопоставяне на действията на киберпрестъпниците се предлага икономическият подход.

ОРГАНИЗИРАНЕ НА БОТНЕТА

Ботнетите се превърнаха в сериозна заплаха за потребителите на Интернет. Битуващият доскоро технически подход за противодействие на ботнетите не се оправда поради ред причини, макар и да не е изчерпал своите възможности. На подобна противоправна дейност, заложена в основата на "сенчестата" икономика на информационните и комуникационните технологии, е необходимо да противопоставим комплекс от действия, обединяващи правното, организационното, техническото и други видове осигуряване. При разглеждането на "сенчестите" информационни технологии според нас основното внимание трябва да бъде пренесено и концентрирано върху икономическите аспекти на противоправната дейност, тъй като се констатира формирането на "сенчеста индустрия". Извличането на максимална по възможност икономическа изгода и печалба е основата, върху която се гради използването на ботнетите.

Освен това законодателната обезпеченост в много страни не съответства на изискванията на днешния ден и не може да осигури сериозно противопоставяне на този вид правонарушения. Макар че практиката за оказване отпор на киберпрестъпниците познава достатъчно успешни примери за достигане до съдебни дела.

Създаването и използването на бот мрежи преследва, преди всичко, икономическа изгода. В резултат на незаконна дейност определени потребители получаваха широк спектър от услуги, които не им се полагат, например незаконно използване ресурсите на Интернет мрежата и много други. Освен това не е тайна, че в Интернет средите получи разпространение сенчестият пазар на продукти и услуги [1,3,9,19-20], чийто обем варира в широк диапазон.

Дейността по създаване и използване на ботнети попада под действието на "Конвенцията на Съвета на Европа за борба с компютърната престъпност" (ноември 2001 година), а също така съответства на раздела за QA кодовете на "компютърните престъпления", използвани от организацията Интерпол. Раздел QA "несанкциониран достъп и прехващане" обединява такива действия като нахлуване в компютърни мрежи, прехващане, кражба на време и други видове несанкциониран достъп и прехващане [10,16].

В дейността на ботнетите се открояват три страни: защищаващ се (действителният собственик на информационната мрежа и информационните ресурси), бот майстор (или бот водещ) и атакуващ.

По такъв начин постоянно се реализират два процеса:

- процес на "зомбиране" или "заразяване" на компютрите (A - като съвкупност от методи и инструменти на кибератаки от страна на нападащите) и

- "обезвреждане" на поразените машини от собствениците на информационни системи (B - като съвкупност от методи и средства за противопоставяне).

Към основния инструментариум на киберпрестъпниците можем да отнесем създаването на ботнети и "зомбиране", използването на логери за клавиатури, разпределени атаки, анализатори на пакети, шпионски програми, троянски програми, компютърни червеи, вирусни механизми и т.н. Трябва да отбележим, че инструментариумът на кибермошениците постоянно се усъвършенства - от използването на механизми за отгатване и разбиване на пароли до многоетапни атаки срещу информационните системи [8].

При $A \succ B$ се извършва съответно разширяване на ботнета. При $A \prec B$ процесът на превземане на мрежата се прекратява и нападащата страна обикновено използва нов инструментариум и усъвършенства методите на кибератака с цел разширяване на ботнета. В случай, че $A \approx B$, може да се говори за фиксиране на точката на насищане. Но даденото равенство не може да продължава дълго време, обикновено се извършва смяна на сценария, като се използва новият инструментариум за нападение и заобикаляне на средствата за защита. Доходът от подобна дейност е непосредствено

пропорционален на стабилността на създадения ботнет и темпа на нарастване на инфектираните машини.

Тайният достъп до компютрите на многобройните потребители и възможността за отдалечен контрол представляват реална заплаха. Реализирането на ботнетите се базира върху използването на специален софтуер, осигуряващ следенето на периодите на активност на заразените системи, което представлява реална опасност преди всичко за електронните платежни системи.

Напоследък доминираща цел на използването на бот мрежите стана организирането на разпределени атаки от типа "отказ от обслужване" (DDoS), разпращането на несанкциониран спам, мошеническата реклама, кражбата на серийните номера на лицензирания софтуер, на входящите пароли на потребителите и на финансова информация (например идентификатори на кредитни карти, номера на банкови сметки и др.). По такъв начин ботнетите се използват от злосторници за постигането на криминални цели от различен мащаб: от разпращането на спам до атаки срещу държавни и търговски мрежи.

Отдалечена атака - несанкционирано информационно въздействие върху информационната система, което се извършва програмирано по каналите за връзка. Обособяват се два подтипа отдалечени атаки. Първият е насочен към инфраструктурата и протоколите на мрежата. Вторият - към телекомуникационните служби, като се използват уязвимите места.

Основните резултати от атаките са следните:

- разширяване на правата за достъп в мрежата;
- изопачаване на информацията;
- разкриване на информацията;
- кражба на Web услуги;
- намаляване производителността на мрежата или блокиране на достъпа до информационните ресурси и много други.

Сложността на извършваната атака се определя от нивото на техническите възможности или общото ниво на знания на атакуващия. Открояват се четири вида подобни възможности:

- ниско - атакуващият пуска разбиващия софтуер, компилира леснодостъпен код или използва познат метод за атака;
- средно - атакуващият използва широко известен метод за нападение, но разгръща атаката с модификация на стандартен набор от средства;
- сложно - атакуващият притежава определен опит, което позволява дълго да скрива присъствието си, като използва собствен написан код;
- много сложно - атакуващият използва неизвестни преди разработки, умело замита следите на атаката и оставя скрити входовете за повторно проникване.

Пълната и достатъчна класификация на отдалечените атаки по видове, в това число такива, като анализ на трафика, подмяна на доверения обект или субект, лъжлив обект, "отказ от обслужване", отдалечен контрол върху станцията в мрежата, е посочена в [2,5,6].

Най-общо разпределената атака се реализира по следния начин - атакуващият:

- компрометира няколко машини, получили название "зомби", а заедно те образуват мрежа, наричана ботнет;
- инсталира на тях софтуер, който впоследствие ще свързва "зомбираните" машини за реализиране на атаките;
- се свързва с машините и обединява възможностите им за реализиране на атаката.

Според сериозността на последиците от реализирането на атаката може да обособим следните нива:

Ниво 1. Включва "отказ от обслужване" и пощенски бомби.

Ниво 2 и 3. Локалните потребители получават за четене и запис достъп до файлове, до които не им е разрешен достъп.

Ниво 4. Това ниво е свързано с външните нарушители, които се опитват да получат достъп до вътрешните файлове на Интранет.

Ниво 5 и 6. Даденото ниво на атаки се характеризира с фатални последици.

Специалистите определят съответните комплекси от действия за противопоставяне на атаките. Конкретно за първо ниво е активна филтрацията на входящите адреси и контактът със сървиз провайдерите на атакуващите. За второ ниво е необходимо да се направи недостъпна и да се вземе под контрол отчетната информация на потребителите. За трето до шесто ниво е необходимо изолиране на мрежовия сегмент, задължително регистриране на всички събития и идентифициране на източниците на атака.

Основните противоправни функции, които изпълняват ботнетите, са следните [3,4,7,9,15,16]:

- разпращане на спам. С помощта на заразени компютри се извършва масово разпращане на електронни писма. Това е най-разпространеният и един от най-обикновените и доходни варианти за експлоатация на ботнетите;

- кибершпионаж и кибершантаж. Ботнетите се използват за извършване на разпределени атаки от типа "отказ от обслужване". Тези действия осигуряват масово претоварване на сайта и водят до неговото блокиране за много кратко време. Съответно, за да се прекрати атаката, киберпрестъпниците искат откуп. Наред с това подобен род действия могат да се разглеждат като средство за информационен натиск върху държавните и търговските структури;

- "измъкване" на информация. Рентабилността на зловредния софтуер за набавяне на информация многократно превишава рентабилността на електронните писма;

- кражба на конфиденциални данни. Специален софтуер позволява да се получат паролите за достъп на потребителите до електронната поща, информационните ресурси и т.н.;

- кражба на софтуер.

Този списък от действия, който съвсем не е изчерпателен, е насочен към "извличане" на пари или създаване на реални условия за потенциални действия с цел превръщане на съответната информация в пари или услуги.

Трябва да се отбележи също, че се наблюдава определено развитие по отношение на крайните цели на киберпрестъпниците. Ако в началото на процесите на развитие на информационните и комуникационните технологии, на широкото внедряване на персоналните компютри, а също така при появата на първите признаци за информационни войни главната цел беше нанасянето на опустошителни щети на собствениците на информационни системи чрез организирането на несанкциониран достъп, унищожаване на информация, нарушаване работата на комуникационното оборудване и софтуера и т.н., в настоящия момент основната цел са "финансовите" стимули и получаване не просто на изгода, а на печалба. Затова в основата на анализа на действията на бот майстора, на атакуващия и използването на средства за противопоставяне трябва да залегне икономическата теория. Основа за оценяването на подобни действия следва да стане съпоставянето на разходите и изгодата (печалбата). И в този случай, ако изгодата от дадения вид дейност превишава разходите, можем да предположим, че действията задължително ще бъдат извършени.

В това направление разработването на икономико-математически модели е призвано да помогне в оценяването на взаимодействието между двете страни - бот майсторите и атакуващите, от една страна, и защитаващата се страна (собствениците на информационни системи и мрежи) от гледна точка определяне размерите на бот мрежите, стойността и изгодата, а също и др. В основата може да залегне комплекс от икономически модели за оценяване стойността на създаването на ботнети [11-13,17,18]. Но предложените модели не отчитат едно съществено обстоятелство - времето на престой на ботнета, което не носи печалба и не компенсира направените разходи.

На свой ред оптимизационният модел представлява доразвит еталонен модел, създаден с помощта на методите за виртуализация и организация на виртуалните машини.

Следва също да отбележим, че с появата на ботнетите възникна и се развива техният "черен" пазар, те се продават, дават се под наем, определят се съответните показатели на "ефективността" (например стойността на създаването на ботнета, размерът на заплащане за изключване уебсайта на жертвата в резултат на извършена атака от типа "отказ от обслужване", стойността на наема на ботнета и др.). Освен това нелегалната индустрия предлага достатъчно широк набор от готови средства - софтуер, готови мрежи и анонимен хостинг. Спадането на доходността от подобни действия според нас трябва да доведе до намаляване привлекателността на процесите по създаване на ботнети и реализиране на разпределени атаки и, в крайна сметка, до тяхното изчезване.

За успешната борба с подобно явление е необходимо "сенчестите информационни предприемачи" да бъдат лишени от възможността да получават печалба и този вид бизнес да стане неефективен. Следва да се създадат такива условия, че участниците в сенчестия Интернет пазар да се сблъскват с повишен риск (технологичен, криминален т.н.).

За бот майстора печалбата се увеличава поради по-големия брой поразени машини, а, от друга страна - необходимо е да се нарасне броят на каналите за поддържане на връзка с поразените машини. Това, на свой ред, значително увеличава възможността той да бъде идентифициран, фиксиран и привлечен към отговорност.

Даже в този случай, когато нападащите извличат сравнително малка печалба, нейният размер прави непривлекателен този сенчест сектор на Интернет технологиите.

Количествени, качествени и стойностни характеристики

Трябва да отбележим, че не съществува официална статистика, която да характеризира дейността на ботнетите. Налице е голямо количество публикации в електронните средства за масова информация, в които са представени експертни оценки за структурата, количествения и качествения състав на "сенчестия" пазар на информационни технологии.

Според нас разпространението и ефективността на ботнетите са пряко свързани с ръста на зловредния софтуер, рязкото увеличаване на външните заплахи, данните за които са посочени в таблици 1-3.

Таблица 1

Динамика на ръста на вредоносните програми

Година	2001	2002	2003	2004	2005	2006	2007	3 тримесечие 2008
Количество вредоносни програми	8821	11136	20731	31726	53950	169689	472621	1315474

Източник: Данни от "Лабораторията на Касперски" за 2008 г.

Таблица 2

Разпределение на вредоносните, рекламни и потенциално опасни програми през 2007 година

Клас	2007	2006	Ръст (в %)
TrojWare	201958	91911	119
WirWare	12416	6282	98
MalWare	5798	4558	27
AdWare	14382	2583	457
RiskWare	2690	-	-

Източник: Данни от "Лабораторията на Касперски" за 2008 г.

Използването на голямо количество "зомбирани" машини заедно с ръста на зловредния софтуер (таблица 2) не само увеличават мощността на атаката, но и усложняват защитата от нея. Наличието на няколко източника на нападение, които използват широк спектър от заплахи, усложнява задачата за блокиране на лъжливия трафик и значително намалява ефективността от проследяването на източника.

Таблица 3

Ръст на количеството външни заплахи в света от 2005 година

Q1 2005	Q1 2006	Q1 2007	Q2 2007	Q3 2007	Q4 2007
100 %	247 %	824 %	1092 %	1314 %	1564 %

Източник: Trend Micro, 2008

Според съобщенията на електронните средства за масова информация през 2008 г. са извършени 190 хиляди атаки и тяхната реализация е донесла около 20 млн. дол. печалба. В таблица 4 са посочени данни, характеризиращи стойностните показатели на ботнет икономиката. Тези данни са получени чрез статистическа обработка от достъпни източници [15,19-20].

Таблина 4

Стойностни показатели, характеризираши ботнет икономиката (щ. дол.)

Показатели	Min значение	Max значение
1	2	3
1. Наемане на ботнет за организирането на 24-часова разпределена атака от типа "отказ от обслужване" (DDoS)	50	1000

Продължение

1	2	3
2. Наемане на ботнет за разпращането на спам (1000 сообщения в минута чрез 100 компютъра, работещи в режим on-line)	2000	-
3. Наемане на малки ботнети	200	700
4. Инфектиране на 1000 компютъра	5	100
5. Кражба на данни относно банкови сметки	1	1500
6. Кражба на данни за откриване на банкова сметка	5-8 (за САЩ)	15-18 (за ЕС)
7. Организиране разпращането на спам	70	1000
8. Наемане на търсеща машина (търсачка)	300	-
9. Инсталиране на adware: - средна цена за инсталиране на adware на 1000 компютъра в Китай - средна цена за инсталиране на adware на 1000 компютъра в САЩ	 3 -	 - 120

Смятаме, че е възможно предлагането на комплекс от икономически модели за оценяване стойността на създаването на бот мрежи, използвайки [11,13-15]. Като основен модел ще разгледаме постановката на задачата за формиране на еталонен модел.

Ще въведем следните променливи:

n^e - минималното количество машини (компютри, сървъри и т.н.), управлявани от бот майстори и атакуващи, необходими за постигането на главната цел (например изключване уебсайта на жертвата). Допълнителното предположение се състои в това, че n^e е величината, която характеризира техническите възможности на ботнета за ефективно провеждане на атаки и се дава под наем срещу определено заплащане;

M - величина на плащането, предназначено за атакуващия, в случай, че е реализирана успешна атака;

P - стойност на наема на ботнета, която се определя на "черните" интернет пазари;

m - стойност на поддържането на канала за връзка (Command and Control Channel) с q "зомбираните" машини в мрежата;

t - количество работни часове на ботнета за един ден;

d - количество работни дни на ботнета за една седмица;

В общ вид задачата за максимизиране на печалбата (без да се взема под внимание използването на виртуалните машини) може да бъде формулирана по следния начин:

1. За атакуващия

$$\max_{n}(\Pr ofit) = M - P*n \quad n \geq n^e \tag{1}$$

2. За бот майстора

$$\max_{k,N}(\Pr ofit) = P*n - m*k - a(N) \qquad k = \frac{n}{q}, \quad N = \frac{n}{\frac{t}{24}*\frac{d}{7}}, \tag{2}$$

където:

N е размерът на типичната ботнет, определян от количеството активни машини;

$a(N)$ - наказателна функция, характеризираща икономическата вреда в случай на откриване, идентифициране на действията и криминалното преследване на бот майстора. Във връзка с това, че вероятността за идентифициране на бот майстора е по-висока, отколкото увеличаването на ботнета, наказателната функция е положителна $(a'(N) \succ 0)$. Освен това количеството активни ботнет машини $(N*\frac{t}{24}*\frac{d}{7})$ трябва да бъде не по-малко от съвкупността (n), тъй като бот майсторът може

да отдава под наем само активните машини, и общото количество канали за управление е достатъчно за поддържането на n машини;

k - брой на управляемите канали за връзка.

По такъв начин за атакуващия стойността на наема за n активни машини се явява управляема променлива, за бот майстора - броят канали за управление (k) и размерът на ботнета (N).

Основни решения за атакуващия и бот майстора могат да бъдат следните:

1. Атакуващият взема под наем n машини за организиране на атаката срещу избрания обект. След реализирането на успешна атака на него му се заплаща M и печалбата му се максимизира при $\mathrm{n} = \mathrm{n}^{\mathrm{e}}$. С други думи, настъпва равновесие между стойността на наема, изгодата за атакуващия и стойността на създаването на ботнета ($M \geq P \geq m$).

2. След пускането на механизма на "зомбиране", осигуряващ функциониране на t часа на ден и d дни в седмицата, размерът на ботнета става равен на $(N = \frac{n^e}{\frac{t}{24} * \frac{d}{7}})$. Едновременно бот майсторът е длъжен да осигури работата на необходимия брой управляеми канали. Вземаме под внимание това, че общият доход $(P * n^e)$ максимизира печалбата и минимизира стойността на поддържането на каналите за връзка $k = \frac{n^e}{q}$.

В този случай без използването на виртуални машини пазарните резултати ще бъдат постигнати - ефективен наем, канали за поддържане и размер на ботнета.

Нека π_b е печалбата на бот майстора и π_a съответно е печалбата на атакуващия. Техните нива могат да бъдат отразени по следния начин:

$$\pi_b = P * n^e - m * \frac{n^e}{q} - a\left(\frac{n^e}{\frac{t}{24} * \frac{d}{7}}\right), \tag{3}$$

$$\pi_a = M - P * n^e. \tag{4}$$

Техните доходи трябва да бъдат положителни. Обединявайки горепосочените изрази, получаваме, че бот майсторът (продавачът) и атакуващият (купувачът) получават своята част от печалбата докато съществува "черен" пазар на информационните мрежи:

$$M \geq P * n^e \geq m * \frac{n^e}{q} - a\left(\frac{n^e}{\frac{t}{24} * \frac{d}{7}}\right). \tag{5}$$

Размерът на печалбата на пазара на бот мрежите или печалбата на бот майстора и атакуващия може да се определи като:

$$\pi_a + \pi_b = M - m * \frac{n^e}{q} - a\left(\frac{n^e}{\frac{t}{24} * \frac{d}{7}}\right). \tag{6}$$

ЗАКЛЮЧЕНИЕ

Представеният материал не изчерпва цялото многообразие от проблеми на сенчестия пазар на информационни технологии. Поставената задача - разглеждане икономиката на сенчестия пазар на информационни и комуникационни технологии може да се смята за изпълнена само при условие, че се изследват комплексно всички сегменти, започвайки от анализа на действията, подпомагащи търсенето на уязвими места в софтуера, организирането на атаки върху информационните ресурси на държавните и търговските системи и завършвайки с формирането на условия за създаване и функциониране на "офшорен кибертероризъм".

Съществуващите теоретични подходи и практически разработки, насочени към създаването на ново научно направление - икономика на информационната сигурност и икономика на сенчестия пазар на информационни технологии, като съставна част от това направление, не отговарят напълно на изискванията на днешния ден, което рязко намалява ефективността на приложната дейност.

Навсякъде специалистите в областта на информационната сигурност отбелязват необходимостта от разработване на методологични основи, които могат да формират базата на икономическия анализ на дейността на информационните системи.

Литература

1. Благодатских В.А., Середа С.А., Поскакалов К.Ф Экономико-правовые основы рынка программного обеспечения. - М.: Финансы и статистика, 2007.
2. Девятин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. -М.: Радио и связь, 2006.
3. Джеймс Л. Фишинг. Техника компьютерных преступлений. -М: НТ Пресс, 2008.
4. Краткий аналитический вопросник по бот-сетям в РФ 2009 год. http://www.securitylab.ru/analytics/370022.php
5. Информационная безопасность открытых систем: В 2 т. Том 1 - Угрозы, уязвимости, атаки и подходы к защите. - М.: Горячая линия-Телеком, 2006.
6. Информационная безопасность систем организационного управления. Теоретические основы: В 2 т. - М.: Наука, 2006.
7. Полный текст отчета McAfee Inc.:
http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf
8. Julia Allen, CERT Guide to System and Network Security Practices, Addison-Wesley, 2001.
9. CISCO: ОТЧЕТ О КИБЕРУГРОЗАХ 2008 ГОДА. HTTP://WWW.SECURITYLAB.RU/NEWS/364919.PHP
10. Interpol Computer Crime Manual. (http://www.surros-cape.org/docs/Computer_Crime_Manual_-_Interpol.pdf)
11. R.Hulthen. Communicating the Economic Value of Security Investments; Value of Security Risk.
12. L.A.Gordon&M.P.Loeb. The Economic of Information Security Investments. ACM Transaction on Information and System Security, 5, No 4, November 2002.
13. Z.Li, Q. Liao, A. Striegel. Botnet Economics: Uncertainty Matters.
14. M.J.G van Eesten, J.M. Baurer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Woring paper 2008/1.
15. Malicious Software (Malware): A Security Threat tj thc Internet Economy. Ministerial Background Report. DSTI/ICCP/REG (2007)5/Final.
16. 2008 CSI Computer Crime & Security Survey.
17. P.Chen, G.Kataria, R.Krishnan. An Economic Analysis of the Strategic Interaction Among Computer Security Attackers.
18. N.Sclavos, P.Souras. Economic Models and Approaches in Information Security for Computer Networks.
19. Security Research Unpick Botnet Economics. (http://www.theregister.co.uk/2009/07/24/botnet economics/
20. Namestnikov Y. The Economics of Botnet. (http://www.viruslist.com/en/analysis?pubid=204792068

ПРИЛОЖНА ИНФОРМАТИКА И СТАТИСТИКА - СЪВРЕМЕННИ ПОДХОДИ И МЕТОДИ

Международна научна конференция

Отг. редактор Емил Мутафчиев
Художник Истилиян Божилов

Даден за печат на 14.07.2010 г.; ПК 35,25;
Формат 8/60/84; тираж 100

ISBN 978-954-644-134-8