MODEL OF PROTECTION MEANS OF PRINTED DOCUMENTS

As of today, the number of protection means in regard to printed documents increases in order to minimize an unauthorized access to information on the tangible medium. There was a need for developing protection models in order to prevent counterfeiting. It was analyzed that the model of protection is formed under the influence of technological factors of document production, as well as combination of protection means and consumer characteristics of the printed document. It was shown that there are six factors influencing consumer characteristics: run length of the document, lifetime of the document, documents' velocity of circulation, intensity of control, intensity of exchange and the available degree of printed document protection. Use of protection models shall make it possible to create the best protection tools for a specific document with its functional features, and calculate the system of effects on the documents' protection levels.

Index words: security level, a printed document, means of protection, technological characteristics, consumer factors.

Шевчук Анатолій Васильович, доктор технічних наук, професор кафедри технології поліграфічного виробництва Національного технічного університету України «Київський політехнічний інститут» Міністерства освіти і науки України, генеральний директор банкнотної фабрики Банкнотно-монетного двору Національного банку України.
E-mail: nazarkevich@mail.ru

Шевчук Анатолий Васильевич, доктор технических наук, профессор кафедры технологии полиграфического производства Национального технического университета Украины «Киевский политехнический институт» Министерства образования и науки Украины, генеральный директор банкнотной фабрики Банкнотно-монетного двора Национального банка Украины.

Shevchuk Anatoly, doctor of technical science, professor at department of Printing Technology National Technical University of Ukraine "Kyiv Polytechnic Institute" Ministry of Education and Science of Ukraine, CEO of Banknote Factory at Mint of the National Bank of Ukraine.

УДК 004.056.53:004.492.3 (045)

ОСНОВНІ ПАРАМЕТРИ ДЛЯ ІДЕНТИФІКАЦІЇ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Андрій Гізун, Владислава Волянська, Вікторія Риндюк, Сергій Гнатюк

Вивчення особистості порушника інформаційної безпеки має велике наукове та практичне значення. Крім того, відповідно до нормативних документів, побудова моделей ймовірних порушників і загроз є важливим етапом у процесі розробки ефективних систем захисту інформації. З цих позицій, формалізація параметрів, які можуть бути використані для ідентифікації порушників, є актуальною науковою задачею. Саме розв'язанню такої задачі і присвячена ця стаття. Чітке визначення повної множини (кортежу) хостових і мережевих параметрів дозволить врахувати особливості атак (зі сторони людей або роботів) і тим самим підвищити ефективність превентивних заходів та систем захисту. Отримані результати можуть бути базисом для побудови системи виявлення вторгнень на основі технології honeypot.

Ключові слова: *порушник інформаційної безпеки, система виявлення порушника, модель порушника, параметри, ідентифікація, робот, кортеж.*

Актуальність. Типова система виявлення порушника (СВП) повинна виконувати такі основні функції [1]: контролювати та аналізувати активність користувачів інформаційних систем (ІС); фіксувати конфігурації системи та вразливості; оцінювати цілісність критичних системних файлів і файлів даних; розпізнавати шаблони активності, що відображають відомі атаки; проводити статистичний аналіз для виявлення аномальної поведінки; розпізнавати порушення політики безпеки користувачем системи. Задачі, що розв'язуються СВП, можна розділити на глобальні та локальні. Глобальні задачі – розпізнавання порушника (Пр) і законного (легітимного) користувача – розв'язання цієї задачі містить такі етапи [1, 2]: збір даних, їх фільтрація, класифікація поведінки – безпосередньо процес розпізнавання Пр, звіт та відгук системи. Як видно з основних функцій та задач СВП одним з найважливіших аспектів їх функціонування є не тільки фіксація самого факту порушення захисту ІС, а і його розпізнавання (ідентифікація).

Постановка завдання. Під *Пр,* у загальному вигляді, можна розглядати особу або групу осіб,

які в результаті навмисних або ненавмисних дій забезпечують реалізацію загроз інформаційній безпеці. У роботі [3] наведено таке визначення – це суб'єкт, дії якого порушують безпеку інформації в комп'ютерній системі. У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель Пр, яка повинна бути адекватна реальному Пр для цієї ІС. *Модель Пр* – абстрактний формалізований або неформалізований опис дій Пр, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. Модель Пр повинна визначати можливу мету Пр та її градацію за ступенями небезпечності для ІС, категорії осіб, з числа яких може бути Пр, припущення про кваліфікацію Пр, припущення про характер його дій [4]. Стосовно ІС Пр можуть бути внутрішніми (з числа персоналу ІС) або зовнішніми (сторонніми особами). Можна виділити три основні мотиви Пр: безвідповідальність, корисливий інтерес, самоствердження. Усіх Пр можна класифікувати у такий спосіб: за рівнем знань про ІС, за рівнем можливостей (використаним методом і засобом), за часом дії, за місцем дії тощо. Проте для ефективної ідентифікації Пр СВП має «знати» набір ключових параметрів. Таким чином, основною ***метою*** цієї роботи є визначення (формалізація) основних параметрів, за змінами яких необхідно спостерігати для ефективної ідентифікації Пр.

Основна частина роботи. Визначення конкретних значень характеристик можливих Пр у значній мірі суб'єктивне. Модель Пр, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду. Кожен вид Пр має бути охарактеризований значеннями параметрів, приведених вище. Відповідно до запропонованої в [5] моделі потенційних дій Пр в ІС, що базується на наведених обґрунтуваннях, *Пр можна класифікувати за такими ознаками:*

1. Стосовно ІС: а) внутрішні, які включають користувачів системи, персонал, що обслуговує технічні засоби, керівників різних рівнів посадової ієрархії, співробітників підрозділу розробки і супроводу програмного забезпечення, технічний персонал, що обслуговує приміщення; б) зовнішні, до числа яких входять представники організацій, взаємодіючих з питань забезпечення життєдіяльності установи, представники конкуруючих установ або особи, що діють за їхнім завданням, відвідувачі, особи, які випадково чи навмисно порушують пропускний режим, будь-які особи за межами контрольованої зони тощо.

2. За мотивами порушення: а) безвідповідальністні особи; б) особи, що мають корисливий інтерес; в) особи, які прагнуть самоствердитись.

3. За рівнем знань про ІС: а) знає функціональні особливості системи; б) має високий рівень знань у сфері програмування, проектування та експлуатації системи; в) має високий рівень знань та досвід роботи з технічними засобами системи.

4. За часом дії: а) у процесі функціонування системи; б) у період неактивних компонентів системи; в) як у процесі функціонування системи так і в період відсутності активності компонентів системи.

5. За рівнем можливостей: а) застосовуючи агентурні методи оволодіння відомостями; б) застосовуючи пасивні засоби; в) використовуючи тільки штатні засоби та недоліки системи захисту для її подолання; г) застосовуючи методи та засоби активного впливу.

6. За місцем дій: а) без доступу на контрольовану територію; б) із контрольованої території без доступу в приміщення; в) усередині приміщення, але без доступу до технічних засобів системи; г) із робочих місць кінцевих користувачів системи; д) з доступом у зону даних; е) з доступом у зону керування засобами безпеки системи.

Загалом, в контексті цієї роботи Пр доцільно розділити на класи, а ті в свою чергу будуть поділені на категорії. Виходячи з природи самого Пр, варто виділити два основних класи: *Пр-людина (ПрЛ)* та *Пр-робот* (або *Пр-бот, ПрБ*). ПрЛ відповідно до своїх можливостей, мотивів та характеру дій вміщує в собі чотири категорії: *зломщик, крекер, спамер* і *дезінформатор*. Аналогічно ПрБ має такі категорії як *спам-бот* і *бот-зломщик*. Одне з центральних понять в галузі Пр інформаційної безпеки – *хакер* (англ. hacker, від to hack – рубати, шматувати) – надзвичайно кваліфікований ІТ-фахівець, людина, яка розуміє самі глибини роботи комп'ютерних систем. Спочатку хакерами називали програмістів, які виправляли помилки в програмному забезпеченні (ПЗ) яким-небудь швидким і далеко не завжди елегантним (в контексті стилю програмування, що використовується у програмі та її загальної структури, дизайну інтерфейсів) або професійним способом. Зараз хакерів дуже часто ототожнюють з комп'ютерними зломщиками – *крекерами* (англ. cracker, від to crack – розколювати, розламувати), однак таке вживання

слова «хакер» некоректне. Іноді цей термін застосовують для позначення фахівців взагалі – у тому контексті, що вони мають дуже детальними знаннями в будь-яких питаннях або мають досить нестандартне і конструктивне мислення. З моменту появи цього слова у формі комп'ютерного терміна (1960-ті роки), у нього з'являлися нові, часто різні значення. Таким чином, хакер – надто загальне поняття і в роботі пропонується розділити його на такі категорії як зломщик та крекер [6].

У роботі під категорією *зломщик* будемо розуміти Пр, який, користуючись переважно власноручно написаними скриптами, зламує захист ІС і порушує конфіденційність інформації, що в ній зберігається, переважно без корисних цілей. Його атака закінчується в момент злому захисту ІС, а в самій ІС він переважно не робить жодних змін і модифікацій (на відміну від крекера).

Крекер (англ. cracker) – тип комп'ютерного зломщика: 1) особа, яка зламує системи захисту (зокрема захисту ПЗ); 2) людина, що займається створенням або доопрацюванням так званих креків; 3) особа, яка зламує комп'ютерні ігри, ПЗ та ін. На практиці також застосовується загальний термін «комп'ютерний зломщик» або «хакер», що теж не є коректним. Результатом роботи крекерів цілеспрямовано є крек, в абсолютній більшості випадків крекер не володіє вихідним кодом програми, а тому програма вивчається зв'язкою дизассемблера і відладчика із застосуванням спеціальних утиліт. Мотиви крекерів переважно корисливі. У роботі будемо вважати, що основна відмінність між крекером і зломщиком полягає в тому, що крекер проводить певні модифікації в системі, не обмежуючись лише зломом чи отриманням необхідної інформації.

Спамер – це Пр, що розповсюджує спам, атакуючи за його допомогою ІС. Спам (англ. spam) – розсилка комерційної та іншої реклами або інших видів повідомлень (інформації) особам, які не виразили бажання їх отримувати. За даними Лабораторії Касперського [7] у 2012 році поштовий спам в Internet розподілився за тематикою таким чином: 18,9% – освіта, 15,7% – відпочинок і подорожі, 15,5% – медикаменти, товари/послуги для здоров'я, 9,2% – комп'ютерне шахрайство, 6,5% – комп'ютери та Internet, 5,2% – репліки елітних товарів, 4,1% – реклама спам-послуг, 2,7% – «інформація для дорослих», 2,2% – нерухомість, 2,2% – юридичні послуги, 1,9% – особисті фінанси, 1,4% – поліграфія. Крім власне почтового спаму виділяють також інші види атак, які можуть здійснюватися подібним чином, а саме DoS і DDoS-атаки – масове розсилання від імені іншої особи з ціллю викликати до нього негативне ставлення, розсилання листів, що містять комп'ютерні віруси (для їхнього початкового поширення), фішинг тощо. Таким чином у нашій класифікації під категорію спамер потрапляють також Пр, що організовують DoS і DDoS-атаки, а також ті, що займаються комп'ютерним шахрайством – фішингом (оскільки методи побудови атак у них практично однакові).

Остання категорія ПрЛ є *дезінформатор* – це особливий вид Пр, що за своїми характеристиками близький до хакера або крекера, але має одну особливість – метою його атак є порушення цілісності і достовірності (інколи й доступності) іформації, що зберігається в ІС.

Категорії в стандартній моделі Пр Таблиця 1

Категорія	Стосовно ІС	Мотив	Рівень знань	Рівень можливостей	Час дії	Місце дії
Зломщик	Зовнішній	Самоствердження	Володіють високим рівнем знань у галузі обчисл. техніки та програмування, проект. та експлуатації ІС	Використовують способи і засоби активного впливу на ІС	Як у процесі функціонування ІС, так і в період активності компонентів ІС	Без одержання доступу на контрольовану територію організації
Крекер	Зовнішній/ Внутрішній	Корисливий мотив				
Спамер	Зовнішній	Корисливий мотив	Володіють інформацією про функціональні особливості ІС, вміють користуватися штатними засобами			
Дезінформатор	Зовнішній/ Внутрішній	Корисливий мотив				

Робот, або *бот,* а також *Internet-бот* (англ. bot, скор. від англ. robot) – спеціальна програма, що виконує автоматично і (або) за заданим розкладом які-небудь дії через ті ж інтерфейси, що й звичайний користувач. При обговоренні комп'ютерних програм термін вживається в основному відносно Internet. Зазвичай боти призначаються для виконання одноманітної і повторюваної роботи з максимально можливою швидкістю (очевидно, набагато вище можливостей людини). Боти знаходять також застосування в умовах, коли потрібна найкраща реакція у порівнянні з мо-

жливостями людини (наприклад, ігрові боти, боти для Internet-аукціонів тощо) або, рідше, для імітації дій людини (наприклад, боти для чатів та ін.) [8, 9]. Шкідливим проявом ботів є їх використання для координації мережних атак на комп'ютери, наприклад, DDoS-і DoS-атак через ботнет. Internet-боти можуть використовуватися для шахрайства типу Клікфрод (Click fraud). Останнім часом стали масовими боти, використовувані в іграх жанру MMORPG. Спам-боти використовуються для поширення по різних ресурсам мережі інформації (зазвичай рекламного змісту).

Виділимо у цьому класі дві категорії: *спам-боти* і *боти зломщики*. *Спам-боти* подібні до ПрЛ спамера, але виконують свої дії автоматично. Основні шкідливі дії ботів цієї категорії: спам-боти, що збирають адреси E-mail з контактних форм і гостьових книг; програми, які завантажили Internet-канал потоком непотрібної інформації (як правило, рекламного характеру); сайти, які збирають інформацію у нешкідливих сайтах, для використання її в автоматично створюваних дорвеях (спеціальні HTML-сторінки, складені для високого позиціонування у пошукових системах за певним ключовим словом); DoS- і DDoS-атаки та ін. До другої категорії відносяться *ботнети* та *комп'ютери-зомбі*. По суті вони містять в собі характеристики хакерів і крекерів, причому організовані повністю в автоматичному порядку. *Ботнет* (англ. botnet, походить від слів robot і network) – це комп'ютерна мережа, що складається з деякої кількості хостів із запущеними ботами – автономним ПЗ. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на пристрій жертви і дозволяє зловмиснику виконувати певні дії з використанням ресурсів зараженого комп'ютера. Зазвичай використовуються для нелегальної діяльності – розсилання спаму, перебору паролів на віддаленій системі, DoS-атак тощо [8, 9].

Щоб розпізнати Пр потрібно порівняти його профіль (тобто його діяльність в ІС) з профілем кожної із категорій загальної моделі Пр. У моделі IDES для характеристики очікуваної діяльності обчислювальної системи використовуються профілі. Параметри діяльності обчислювальної системи, використовувані для побудови профілю, можуть змінюватися в залежності від типу діяльності ІС, яка контролюється. Параметри для ідентифікації поділяють на два типи: *хостові* (табл. 2) і *мережеві* (табл. 3), характеристики яких описані нижче. У більшості випадків звичайними типами інформації, присутніми в профілях на хостовому рівні, є [10]:

1) Вхідна діяльність. Для даного користувача або системи профілі можуть характеризувати звичайне число входів у певний період часу протягом дня, передбачуваний найбільш ранній час входу, передбачувану максимальну тривалість входу і т.д. Практика показала, що такі параметри найбільш типові для більшості обчислювальних операційних середовищ. Наприклад, для деяких операційних середовищ спроба користувачів зареєструватися в системі о 4-й годині ранку не є нормальною, тоді як в інших вона може вважатися звичайною дією.

2) Параметри виконання. Профілі також можуть встановлюватися у залежності від передбачуваного типу використання ресурсів, які повинна підтримувати певна обчислювальна система. Серед таких профілів, як правило, повинні бути статистики використання процесорного часу, пам'яті та інших ресурсів. Це ще один параметр, який зазвичай регулярний і передбачуваний. У середовищі виконання канцелярських звітів, наприклад, програма, що викликається, яка займає більше 10 хвилин процесорного часу, повинна розглядатися як ненормальна, в той час як в науковому операційному середовищі вона може бути цілком нормальною. Параметри виконання у системі виявлення Пр дають засоби для можливого відображення цього типу зловмисної діяльності.

3) Доступ до файлів. Можна створити профілі частоти читання і запису певних файлів, числа відмов на запити читання або запису певних файлів і профілі інших параметрів доступу до файлів. Цей параметр може бути менш передбачуваним, але певні файли можуть бути помічені як недоступні для звичайних користувачів. Наприклад, якщо звичайний користувач намагається що-небудь записати в файл паролю, то це можна розглядати як ненормальну поведінку. У більшості операційних середовищ копіювання файлу паролю повинно вважатися підозрілою діяльністю. Залежно від типів передбачуваних атак можна запропонувати такі методи аудиту для СВП хоста, що наведені в роботах розробників системи NIDES [1, 11]:

а) аудит входу в систему – збирає дані про те, хто, коли і як увійшов в систему. При цьому доцільно фіксувати: ім'я користувача, що увійшов в систему; найменування терміналу або віддаленого хоста, з якого був здійснений вхід в систему; час входу і виходу користувача.

б) аудит процесів – збирає дані про те, які сервіси системи були використані. При цьому доціль-

но фіксувати: умови виконання (наприклад, чи використовуються права суперкористувача) процесу; значення, що повертається процесом при завершенні; ім'я користувача і групи; термінал, з якого запущений процес; час виклику процесу; час, проведений в режимі користувача; час, проведений в режимі ядра; загальний час виконання; середня використана пам'ять; кількість оброблених символів; кількість зчитаних-записаних блоків інформації; ім'я команди для запуску процесу.

3. Аудит помилок та адміністративних даних.

Аналогічно, наша система повинна моніторити певні параметри діяльності ІС, фіксувати їх і здійснювати ідентифікацію Пр.

Хостові параметри для ідентифікації Пр та їх характеристика Таблиця 2

Параметр	Нечіткість	ПрЛ				ПрБ	
		Дезінформатор	***Спамер***	***Крекер***	***Хакер***	***Спам-бот***	***Бот-зломщик***
UID	-	+	-	+	+	-	+
Tlog	+	З певною ймовірністю залежно від часу доби	-	З певною ймовірністю залежно від часу доби	З певною ймовірністю залежно від часу доби	-	З певною ймовірністю залежно від часу доби
Nlog	+	Вище середнього	-	Вище середнього	Вище середнього	-	Висока
TSlog	+	Вище середнього	-	Вище середнього	Вище середнього	-	Вище середнього
I	+	В межах норми	В межах норми	В межах норми	В межах норми	Вище норми	Вище норми
CPU	+	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми
MUse	+	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми
NEF	+	Не в межах норми	-	Не в межах норми	Не в межах норми	-	Не в межах норми
AtEF	-	Скрипти та PHP-скрипти	PHP-скрипти	Виконуючі файли	Скрипти	PHP-скрипти	Скрипти
NEr	+	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми	Вище норми
RTPr/F	+	Відрізняється від типового часу	Відрізняється від типового часу	Відрізняється від типового часу	Відрізняється від типового часу	Відрізняється від типового часу	Відрізняється від типового часу
UPr	-	Присутні	Присутні	Присутні	Присутні	Присутні	Присутні
TrFin	-	Присутня	Присутня	Присутня	Переважно відсутня	Присутня	Переважно відсутня
ModF	-	Присутня	Відсутня	Присутня	Переважно присутня	Відсутня	Переважно присутня
TrFout	-	Відсутнє	Відсутнє	Переважно присутнє	Присутнє	Відсутнє	Присутнє
KS	-	Фіксується	Фіксується	Фіксується	Фіксується	Не фіксується	Не фіксується

Розглянемо більш детально ці параметри: *1) Ім'я користувача при вході (UID).* У базі даних СВП або honeypot, на основі якого будується ця система, повинен бути визначений і збережений перелік імен користувачів (логінів), яким дозволено використовувати ресурси ІС (тобто які є авторизовані). Будь-які інші імена користувачів, що не ввійшли у цей перелік, вважаються не авторизованими і їх поява свідчить про несанкціонований вхід у систему. Цей параметр є чітким оскільки поява не властивого логіну однозначно вказує на Пр. Проте спамери, спам-боти і боти-шукачі зазвичай не потребують авторизації в системі і тому факт проникнення їх в систему за цим параметром переважно визначити неможливо. *2) Час входу у систему (Tlog).* Параметр заснований на тому, що активність ІС і користувачів цих систем залежить від часу доби. Зазвичай більша активність користувачів щодо входу в систему виявляється в денний час, менша – в нічний, але можлива інша статистика, яка визначається режимом роботи організації, до яких належать ІС. Природа цього параметра нечітка, адже неможливо однозначно зробити висновок про нелегальну актив-

ність Пр. Так в організаціях з часом роботи з 08:00 до 16:00 імовірність того, що користувач, який авторизувався – це Пр, найнижча в 08:00 і з часом зростає, досягаючи максимуму в години після 16:00. Однак, слід відмітити, що в концепції honeypot-технологій цей параметр дещо втрачає свою вагу, так як будь-яка активність на них вважається зловмисною. *3) Частота запитів на вхід у систему (Nlog).* Зрозуміло, що найвища частота запитів на вхід буде відмічатися при атаках системи ботами (зокрема ботами-зломщиками, так як спамери не потребують входу у систему). ПрЛ теж відзначається підвищеною частотою запитів внаслідок намагання обійти захист і теоретичного припущення що він не володіє легітимним логіном та паролем, тому буде змушений робити як мінімум декілька спроб. Причому чим більше число спроб, тим більша ймовірність що в ІС дійсно намагається ввійти Пр. Зрозуміло, що цей параметр теж є нечітким. *4) Час затрачений на вхід в систему (TSlog).* Параметр, який тісно пов'язаний з попереднім. Час, затрачений Пр, у більшості випадків більший за час, затрачений легітимним користувачем. Але він є нечітким, оскільки не дає змоги провести однозначну ідентифікацію. *5) Інтенсивність дій (I).* Тут розуміється кількість будь-яких дії користувача, що включають в себе вхід/вихід з системи, передачу, зміну, копіювання файлів, запуск/припинення процесів та ін. в одиницю часу. Інтенсивність може не відрізнятися в ПрЛ і в легітимного користувача, однак у ботів вона значно вища, тому найбільш суттєва для ідентифікації та розмежування категорій людина-бот. Хоча значне перевищення норми вказує на діяльність неавторизованих автоматичних систем-Пр (ботів), проте I – нечіткий параметр, оскільки нормальну величину показника інтенсивності визначити дуже важко. *6) Процесорний час/завантаженість процесора (CPU).* Оскільки кількість активних процесів на honeypot-системах мусить бути мінімальною, то будь-яке збільшення навантаження є ознакою діяльності Пр в системі. У реальних ІС імовірність того, що активність спричинена саме Пр дещо нижча, а, зрозуміло, нормальна величина процесорного часу вища. Проте цей параметр все одно можна ефективно використовувати для ідентифікації факту порушення в системах виявлення вторгнень і СВП. Оскільки однозначну відповідь про Пр за цим параметром дати неможливо, в першу чергу через можливу діяльність вірусів, то процесорний CPU – нечіткий параметр. *7) Об'єм завантаженої оперативної пам'яті (MUse).* Аналогічний за змістом до попереднього і також є нечітким. *8) Кількість виконуваних файлів (NEF).* Також входить в групу нечітких параметрів. Факт дій зловмисника по цьому параметру визначається відхиленням від норми. Так, у кожній організації, відповідно до політики безпеки та посадових обов'язків кожен легітимний користувач може використовувати певні файли в заданий момент, причому одночасне використання одразу багатьох файлів практично виключається. Це дає змогу виявити як зовнішнього, так і внутрішнього Пр, але з певною ймовірністю. *9) Тип використовуваних файлів при атаці (AtEF).* Якщо був помічений нещодавно змінений чи створений файл, який ідентифікується як скрипт – то маємо справу з хакером, людиною, що у вищій мірі володіє комп'ютерною грамотністю і здатна здійснити за допомогою виявленого нами скрипту подальші злами систем. Якщо помічений файл є виконуючим файлом, то згідно з визначенням «… результатом роботи крекера є … модифікована («крекнута» або «зламана») програма з потрібною функціональністю» можемо судити, що людина, яка зламала захист сервера, є крекером. І врешті-решт випадок, коли ми знаходимо PHP-скрипт, однозначно говорить про зломщика, що працює в мережі Internet. За даними сучасних досліджень найбільша кількість, серед розглянутих категорій зловмисників, DDoS-рів та спамерів. Дезінформатор може використовувати декілька видів файлів, переважно це скрипти та PHP-скрипти. Оскільки результат застосування параметру дає однозначну відповідь про наявність Пр та його клас, то параметр чіткий. *10) Кількість збоїв та помилок (NEr).* Цей параметр є нечітким, оскільки збої та помилки можуть відбуватися під час роботи як авторизованого користувача так і Пр. Проте при частому повторені збоїв чи помилок можна зробити висновок з певною долею імовірності що система атакована. У цю групу входить широкий спектр подій від помилок при авторизації до збоїв при виконанні певних процесів або файлів. При активній роботі Пр, незалежно від його класу та категорії, частота появи несправностей буде дещо вищою. Слід також відмітити, що цілком можливо при ідентифікації ПрБ ця частота буде ще вищою. *11) Час виконання процесу/файла (RTPr/F).* Досліджуючи статистику роботи ІС різних підприємств та організацій легко помітити, що залежно від специфіки роботи час, затрачений на виконання певної операції є приблизно однаковий для однотипних ІС та їх задач. У honeypot-системах в основному виконуються системні

процеси, тобто ті, що підтримують роботу самого honeypot, або процеси адміністратора, що запускаються в певний час на деякий період. Таким чином, при ідентифікації таких процесів можна зробити висновок про атаку системи Пр. Оскільки, такий стан речей може бути спричинений халатністю працівника, то висновок є неоднозначний і відповідно параметр носить нечіткий характер. *12) Невластиві процеси (UPr).* Відповідно до концепцій СВП і honeypot-систем в ІС повинен вестись постійний моніторинг виконуваних процесів. Так на протязі часу роботи системи можуть формуватися так звані зліпки системи, які фіксують всю активність на хості або створюються списки процесів та їх характеристик, що були запущені. У випадку появи невластивого процесу в роботі ІС, тобто такого який протягом тривалого часу не запускався взагалі або запускався обмежено невелику кількість раз, наша СВП відразу відмічає факт появи Пр. Оскільки в такому разі імовірність правильного підняття тривоги практично дорівнює «1», то параметр можна віднести до чітких. *13) Передача файлу в систему (TrFin), зміна файлів (ModF), копіювання/передача фалів з системи (TrFout)* – це група чітких параметрів. Будь-які дій з файлами властиві кожній атаці, але ті дій, які переважають під час атаки, визначають клас та категорію Пр. Так, наприклад, при спам-атаці зазвичай відзначають передачу файлів у систему, проте їх зміна чи передача з системи переважно відсутні. Аналогічно ідентифікують інші категорії Пр. *14) Натиснення клавіш клавіатури (KS).* Для виявлення атак у цій технології використовується моніторинг за натисканням користувача на клавіші клавіатури. Основна ідея - послідовність натискань користувача задає патерн атаки. Недоліком цього підходу є відсутність досить надійного механізму перехоплення роботи з клавіатурою без підтримки операційної системи, а також велика кількість можливих варіантів представлення однієї і тієї ж атаки. Крім того, без семантичного аналізатора натискань різного роду псевдоніми команд можуть легко зруйнувати цю технологію. Оскільки вона спрямована на аналіз натискань клавіш, автоматизовані атаки, які є результатом виконання програм зловмисника, також можуть бути не виявлені. Але саме цей факт є для нас найбільш корисним в процесі ідентифікації Пр і віднесені його до класу людей або роботів. Цей параметр є однозначним, отже також віднесений до групи чітких.

Мережеві СВП працюють з мережевим трафіком і виявляють атаки, пов'язані з низькорівневим впливом на мережеві протоколи, і можуть виявити атаки на кілька хостів мережі. Мережеві СВП будується на основі інтелектуального аналізатора трафіку, обробляючого кожен фрейм даних, що проходить через нього, на предмет пошуку в ньому заборонених сигнатур, що позначають атаки. Мережеві дані, мережевий трафік отримують від мережевого адаптера функціонуючого в promiscuous моді (тобто приймаючи всі пакети в мережі).

Мережеві параметри для ідентифікації Пр та їх характеристика Таблиця 3

Параметр	**Нечіткість**	**ПрА**				**ПрБ**	
		Дезінформатор	***Спамер***	***Крякер***	***Хакер***	***Спам-бот***	***Бот-зломщик***
ARP-запит	-	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному
IP-фрагмент	-	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному
ICMP-повідомлення	-	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному
TCP-пакет	-	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному	Не відповідає дозволеному

Перерахуємо дані аудиту, які необхідно знімати для виявлення віддалених атак, з характеристиками сімейства протоколів TCP/IP [1, 11]: *ARP запит* моніториться за такими параметрами: IP адреса джерела; апаратна адреса джерела; мережевий інтерфейс, що обмежує ARP запит. *IP-фрагмент:* адреса джерела; адреса приймача; поле протоколу; поле зміщення; довжина; довжина заголовка; MF біт; ідентифікація. *ICMP повідомлення:* IP адреса джерела; IP адреса приймача; ICMP

поле типу; ICMP ідентифікатор; ICMP номер послідовності. *TCP пакет:* IP адреса джерела; IP адресу приймача; TCP порт джерела; TCP порт приймача; біт коду TCP.

Усі перераховані мережеві параметри за умови правильного налаштування політики міжмережевої взаємодії чітко вказують на атаку, а тому відносяться до групи чітких. Описані у роботі параметри (як мережеві, так і хостові) утворюють кортеж виявлення і ідентифікації Пр:

$$DIO = < UID, Tlog, Nlog, TSlog, I, CPU, MUse, NEF, AtEF, NEr, RTPr/F, UPr, TrFin, ModF, TrFout, KS, ARP, IP, ICMP, TCP >.$$

Значення елементів (а вірніше, їх зміна) цього кортежу дають змогу виявити факт проникнення Пр в ІС, а також тип Пр: для ПрЛ – зломщик, спамер, дезінформатор і крекер, а для ПрБ – бот-зломщик і спам-бот.

Висновки. Таким чином, у цій роботі визначено кортеж параметрів (хостових і мережевих) для ідентифікації Пр (чіткого визначення типу – тобто ПрЛ чи ПрБ). Формалізація таких параметрів дозволяє врахувати особливості атак на ІС і підвищити ефективність превентивних заходів та систем захисту інформації. У подальших дослідженнях ці результати можуть бути базисом для побудови ефективної системи виявлення вторгнень на основі технології honeypot.

ЛІТЕРАТУРА

[1]. Корт С.С. Структура систем обнаружения нарушителя [Електронний ресурс]: стаття / С.С. Корт. – Режим доступу: http://www.ssl.stu.neva.ru/sam/

[2]. Denning D.E. An Intrusion-Detection Model / Dorothy E. Denning // IEEE Transactions On Software Engineering. – February 1987. – Vol. SE-13, No. 2. – P. 222-232.

[3]. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670 с.

[4]. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.

[5]. Головань С.М. Базові вимоги до побудови моделі загроз інформаційних систем / С.М. Головань // Інформаційна безпека. – 2009. – №1. – С.17-25.

[6]. Hacker [Електронній ресурс]: стаття словника // Энциклопедическом словаре хакера (Jargon File). – Режим доступу: http://www.catb.org/~esr/jargon/html/H/hacker.html

[7]. Гудкова Д. Спам в 2012 году [Електронний ресурс]: стаття / Д. Гудкова. – Режим доступу: http://www.securelist.com/ru/analysis/208050782/Spam_v_2012_godu

[8]. Камлюк В. Ботнеты [Електронній ресурс]: стаття / Виталий Камлюк. – Режим доступу: http://www.securelist.com/ru/analysis?pubid=204007610.

[9]. Ботнеты: беда, откуда не ждали [Електронній ресурс]: стаття // UPgrade. – Июль 2012. – №584. – Режим доступу: http://www.upweek.ru/botnety-beda-otkuda-ne-zhdali.html.

[10]. Ptacek Thomas H. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection / Thomas H. Ptacek, Timothy N. Newsham. – Secure Networks, Inc, 1998. – 63 с.

[11]. Корт С.С. Методы обнаружения нарушителя [Електронній ресурс]: стаття / С.С. Корт. – Режим доступу: http://www.ssl.stu.neva.ru/sam/

REFERENCES

[1]. Kort S.S. Struktura sistem obnaruzheniya narushitelya [Electronic resource]: stattja / S.S. Kort. – Mode of access: http://www.ssl.stu.neva.ru/sam/

[2]. Denning D.E. An Intrusion-Detection Model / Dorothy E. Denning // IEEE Transactions On Software Engineering, February 1987, Vol. SE-13, No. 2, P. 222-232.

[3]. . Babak V.P. Informatsijna bezpeka ta suchasni merezhevi tekhnologii: Anglo-ukrayins`ko-rosijs`kyj slovnyk terminiv / V.P. Babak, O.G. Korchenko, K.: NAU, 2003, 670 s.

[4]. ND TZI 1.4-001-00. Typove polozhennia pro sluzhbu zakhystu informatsii v avtomatyzovanii systemi.

[5]. Golovan` S.M. Bazovi vymogy do pobudovy modeli zagroz informatsijnykh system / S.M. Holovan` // Informatsijna bezpeka, 2009, №1, S.17-25.

[6].Hacker [Electronic resource]: stattja slovnyka // Entsiklopedicheskiy slovar hakera (Jargon File). Mode of access: http://www.catb.org/~esr/jargon/html/H/hacker.html

[7]. Gudkova D. Spam v 2012 godu [Electronic resource]: stattja / D. Gudkova, Mode of access: http://www.securelist.com/ru/analysis/208050782/Spam_v_2012_godu

[8]. Kamlyuk V. Botnety [Electronic resource]: stattja / Vitaliy Kamlyuk., Mode of access: http://www.securelist.com/ru/analysis?pubid=204007610.

[9]. Botnety: beda, otkuda ne zhdali [Electronic resource]: stattja // Upgrade, July 2012. – №584. – Mode of access: http://www.upweek.ru/botnety-beda-otkuda-ne-zhdali.html.

[10]. Ptacek Thomas H. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection / Thomas H. Ptacek, Timothy N. Newsham. – Secure Networks, Inc, 1998, 63 с.

[11]. Kort S.S Metody obnaruzheniya narushitelya [Electronic resource]: stattja / S.S. Kort. – Mode of access: http://www.ssl.stu.neva.ru/sam/

ОСНОВНЫЕ ПАРАМЕТРЫ ДЛЯ ИНЕДТИФИКАЦИИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изучение личности нарушителя информационной безопасности имеет большое научное и практическое значение. Кроме того, в соответствии с нормативными документами, построение моделей вероятных нарушителей и угроз является важным этапом в процессе разработки эффективных систем защиты информации. С этих позиций, формализация параметров, которые могут быть использованы для идентификации нарушителей, является актуальной научной задачей. Именно решению такой задачи и посвящена эта статья. Четкое определение полного множества (кортежа) хостовых и сетевых параметров позволит учесть особенности атак (со стороны людей или роботов) и тем самым повысить эффективность превентивных мер и систем защиты. Полученные результаты могут быть базисом для построения системы обнаружения вторжений на основе технологии honeypot.

Ключевые слова: нарушитель информационной безопасности, система обнаружения нарушителя, модель нарушителя, параметры, идентификация, робот, кортеж.

MAIN PARAMETERS FOR INFORMATION SECURITY INTRUDER IDENTIFICATION

Studying of the person of information security intruder has a great scientific and practical importance. In addition accordingly to normative documents intruders and threats models development is important stage in development of effective information security systems. From this viewpoint parameters formalization for intruder identification is an actual research problem. The solving of this problem is a subject of the paper. Definition of complete set (cortege) of host and network parameters can give a possibility to consider features of attacks (from people or robots) and to increase preventive measures & security systems efficiency. Given results can be the basis for intrusion detection systems based on honeypot-technology development.

Key words: information security intruder, intruder detection system, intruder model, parameters, identification, robot, cortege.

Гізун Андрій Іванович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету,
E-mail: caesar07@meta.ua
Гизун Андрей Иванович, асистент кафедры безопасности информационных технологий Национального авиационного университета
Gizun Andriy, Assistant of Academic Department of IT-security, National Aviation University

Волянська Владислава Вікторівна, IT-менеджер Apogeum Sp. z o.o. Poland.
E-mail: volyanska.vladyslava@gmail.com
Волянская Владислава Викторовна, ИТ-менеджер Apogeum Sp. z o.o. Poland.
Volyanska Vladyslava, IT-manager Apogeum Sp. z o.o. Poland

Риндюк Вікторія Олександрівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій, математики та засобів дистанційного навчання П'ятигорського державного лінгвістичного університету
E-mail: vika012001@mail.ru
Рындюк Виктория Александровна, кандидат технических наук, доцент, доцент кафедры Информационных технологий, математики и средств дистанционного обучения Пятигорского государственного лингвистического университета
Ryndyuk Victoria, Ph.D., Assistant Professor, Associate Professor at Department of Information Technology, Mathematics and tools of distance learning Pyatigorsk State Linguistic University

Гнатюк Сергій Олександрович, к.т.н., доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
Гнатюк Сергей Александрович, к.т.н., доцент кафедры безопасности информационных технологий Национального авиационного университета
Sergiy Gnatyuk, PhD, Associate Professor of the Academic Department of IT-security, National Aviation University.