Кібернетична безпека

УДК 004.023; 004.421.2

В.В. Бєрковський, О.С. Безсонов

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

АНАЛІЗ ТА КЛАСИФІКАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ

В статті аналізуються загрози та класифікує методи виявлення вторгнень в інформаційну систему. Виявлені недоліки пов'язані зі структурою СВВ та недоліки реалізації методів виявлення. Для підвищення ймовірності виявлення атак на ІС найперспективнішим буде використання комбінованого методу, а також створення уніфікованої СВВ для захисту як комп'ютерів так і мобільних пристроїв. Визначені подальші напрямки вдосконалення пов'язані з усуненням недоліків сучасних СВВ. Використання сигнатурного методу та методу виявлення аномалій забезпечують додатковий рівень захисту інформаційної системи, доповнюючи "традиційні" засоби захисту для мобільних пристроїв.

Ключові слова: *системи виявлення, системи вторгнення, вторгнення, мережі, сигнатури, системні аномалії, інформаційна атака.*

Вступ

Чим далі людство просувається по інформаційному шляху розвитку тим більша потреба в інформаційних ресурсах.

Інфраструктура сучасного життя, всі аспекти людської активності, гармонійна взаємодія соціальної, природної та економічної систем не можуть існувати без інформаційних ресурсів.

Але як і будь-яка інша система, система інформаційних ресурсів піддається негативним впливам і загрозам як із зовні так і зсередини.

1. Поняття загрози та безпеки інформації

Загроза - потенційно можлива подія (вплив, процес або явище), яке може привести до нанесення шкоди безпеці автоматизованих систем (АС). Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту АС [1].

Класифікація загроз інформаційній безпеці АС обумовлена тим, що в сучасних АС інформація, яка збережена і та, що обробляється піддаються впливу надзвичайно великого числа факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тому для системи, яка захищається, зазвичай визначають перелік класів загроз, а не повний перелік загроз. Більш детальна класифікація можливих загроз інформаційній безпеці АС зображена на рис. 1.

При цьому важливими аспектами є - забезпечення безпеки й цілісності системи, захист цілісності інформації, мінімізація втрат, якщо інформація буде модифікована або зруйнована.

Під інформаційною безпекою розуміється захищеність інформації від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформації [2].

Розрізняють чотири рівні захисту інформації [3]:

Запобігання - доступ до інформації та технології надається тільки для персоналу, який отримав допуск від власника інформації;

Виявлення - забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;

Обмеження - зменшується розмір втрат, якщо злочин все-таки відбулося, не дивлячись на заходи щодо його запобігання та виявлення;

Відновлення - забезпечується ефективне відновлення інформації при наявності документованих і перевірених планів з відновлення.

Аналіз операційних систем, що до захищеності від несанкціонованих впливів. На даний момент найбільшого ризику піддаються операційні системи (ОС) сімейства Windows, що викликано великою кількістю шкідливих програм саме під цю платформу. Це, є наслідком великої популярності ОС цього сімейства, також як і великою кількістю засобів розробки, в тому числі безкоштовних, і навіть «інструкцій з написання вірусів». Інші платформи такі як Linux і Mac OS X менш схильні до ризиків завдячуючи своїй архітектурі.

Останнім часом все більшого розповсюдження набувають платформи для мобільних пристроїв.

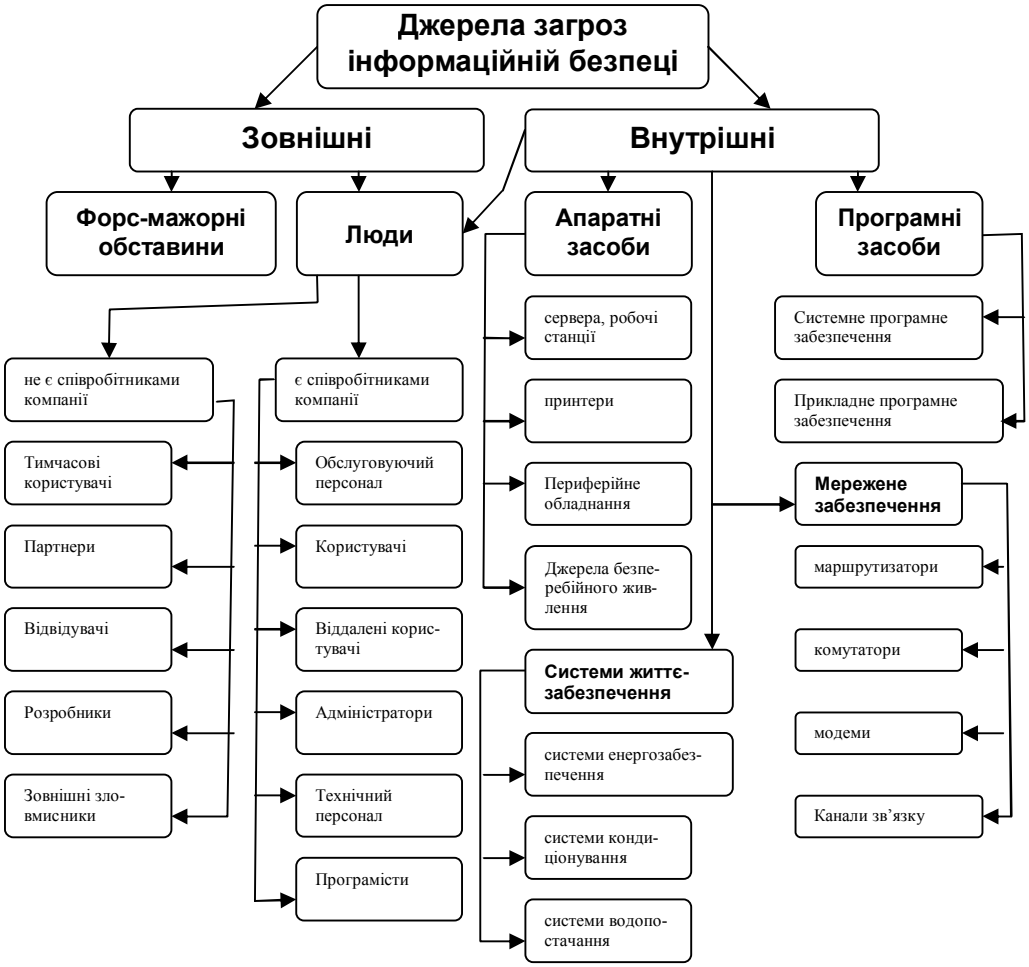

Рис. 1. Класифікація можливих загроз інформаційній безпеці АС

Сьогодні є безліч платформ для смартфонів і планшетів: Android, iOS, RIM BlackBerry, Symbian, мобільні варіанти Windows. Користувачі пристроїв з такими ОС є потенційними об'єктами зараження шкідливим програмним забезпеченням.

Виробники роблять певні зусилля для захисту даних мобільних пристроїв, у першу чергу мова йде про дані в системних розділах. Системна пам'ять мобільних пристроїв, як правило невелика, тому деяким програмам дозволяється зберігати дані за її межами.

Всупереч те що різноманіття платформ є перешкодою для появи спільних загроз, більша частина пристроїв дозволяє зберігати дані на зовнішній карті пам'яті з файловою системою FAT. Ця система була розроблена ще в 1976 році і не має власних механізмів ефективного захисту даних, однак вона поширена настільки, що вже стала стандартом де-факто для носіїв малої і середньої ємності [4].

Дані будуть втрачені у разі загублення або крадіжки пристрою, або через додатки подвійного призначення, що мають доступ до карти пам'яті, які збирають дані з файлової системи та записують розмови, наприклад - Android System Messenger. Користувачі встановлюють програми та ігри на пристрої десятками, рідко вчитуючись у список дозволів і звично натискаючи «згоден» і «встановити».

Навіть якщо виключити установку на мобільні пристрої неперевірених програм, зберігання даних у відкритому вигляді залишиться основною вразливістю мобільних пристроїв. Це може реалізуватися при виконанні типових сценаріїв випадкового або несанкціонованого доступу, а також внаслідок втрати, крадіжки пристрою або картки пам'яті.

Історично, найбільш відпрацьований, але працює тільки з платформами одного виробника інструментарій управління мобільними клієнтами міститься в RIM BlackBerry, що досягається в першу чергу за рахунок реалізації в цьому продукті як клієнтську, так і серверну частини комунікаційної з базовим функціоналом управління.

Сьогодні ринок повернувся в бік Android і Apple iOS, що змусило шукати компромісне універсальне рішення, що уступає багатовендорним стосовно до відповідних пристроїв, але дозволяє централізувати управління і захист різних платформ [5]. Прикладом такого рішення що об'єднав функціонал керування і захисту мобільних пристроїв, є LANDesk Management Suite з компонентом LANDesk Mobility Manager.

2. Аналіз розвитку методів боротьби із несанкціонованим доступом до операційних систем

Виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак. Вже в 1984 році Фред Коен заявив, що кожне вторгнення виявити неможливо і ресурси, необхідні для виявлення вторгнень, будуть рости разом зі ступенем використання комп'ютерних технологій [6].

Найбільш поширеними є, так звані локальні і мережеві «Системи виявлення вторгнень» (СВВ). Локальна СВВ передбачає, що система виявлення встановлюється на кожному окремому комп'ютері. Мережева СВВ збирає пакети, що надходять в мережу через один пристрій і аналізують їх, перш ніж пересилати заданим вузлів. Мережеві СВВ сьогодні вважаються менш ефективними, чим більша кількість вузлів в мережі тим важче стає забезпечення надійної фільтрації пакетів і, як наслідок, захист комп'ютерів в мережі.

Системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем і використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки, що спрямовані проти вразливих сервісів, атаки, які передбачають підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

4 листопада 1983 був винайдений перший комп'ютерний вірус [6]. Фред Коен у той час ще аспірант одного з американських університетів, написав першу програму-вірус, яка здатна до саморозмноження та паразитичного поширення по мережах. На презентації своєї докторської дисертації, яка була присвячена проблемі забезпечення безпеки комп'ютерних систем Коен представив першу програму-вірус. Особливої загрози програма Коена не становила, оскільки експеримент був контрольованим і не мав далекосяжних цілей.

На сьогоднішній день виділяють і рекомендують до застосування, в тому числі, і при побудові системи захисту три групи методів виявлення атак:

- сигнатурні методи;
- методи виявлення аномалій;
- комбіновані методи (використовують спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій).

Іншими словами, виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак.

2.1 Сигнатурні методи. Сигнатурні методи описують кожну атаку особливою моделлю або сигнатурою, в якості якої можуть застосовуватися рядок символів - семантичний вираз на спеціальній мові, використанням спеціалізованої бази даних формальна математична модель і т. д. Сутність сигнатурного методу в наступному: у вихідних даних, зібраних мережевими і хостовими датчиками системи виявлення вторгнення (СВВ) з сигнатур атак, виконується процедура пошуку сигнатури атаки. Перевага даних методів - висока точність визначення факту атаки, а очевидний недолік - неможливість виявлення атак, сигнатури яких ще не визначені [7].

Серед сигнатурних методів виявлення атак найбільш поширений метод контекстного пошуку, який полягає в виявленні у вихідній інформації певної безлічі символів. Так, для виявлення атаки на Web-сервер, що спрямована на отримання несанкціонованого доступу до файлу паролів, проводиться пошук послідовності символів "GET * / etc / passwd" у заголовку HTTP-запиту. Фрагмент "cwd ~root" в FTP-сеанс однозначно визначає факт обходу механізму аутентифікації на FTP-сервері і спробі перейти в кореневий каталог FTP-сервера. Іншим прикладом є виявлення аплетів Java в мережевому трафіку на основі шістнадцятирічного фрагмента "CA FE BA BE". Ці ж сигнатури дозволяють виявляти троянських коней, якщо останні використовують стандартні значення портів. Наприклад, троян NetBus, як це вже описувалося у третьому номері BYTE за 2016 рік, визначається по використанню 12345-го і 12346-го портів, а троян BackOrifice - 31337-го порту [6].

Для розширення функціональних можливостей контекстного пошуку в деяких випадках використовуються спеціалізовані мови, що описують сигнатуру атаки. Нижче наведено приклад сигнатури атаки Land, описаної за допомогою мови N-code системи NFR.

```
filter pptp ip ()
{
# Если IP-адрес отправителя пакета
# данных Совпадает с IP-адресом
# получателя, то в журнал записывается
# информация об атаке Land
  if (ip.src == ip.dest)
  {
    system.time, eth.src, ip.src, sth.dst to land_recrdr;
  }
}
```

За допомогою контекстного пошуку ефективно виявляються атаки на основі аналізу мережевого трафіку, оскільки даний метод дозволяє найбільш точно задати параметри сигнатури, яку необхідно виявити в потоці вихідних даних.

У ряді академічних СВВ були реалізовані ще два сигнатурних методи: метод аналізу станів і метод,

який базується на експертних системах. Метод аналізу станів або контролю частоти подій заснований на формуванні сигнатури атак у вигляді послідовності переходів інформаційної системи ІС з одного стану в інший. По суті, кожен такий перехід визначається по настанню в ІС певної події, а набір цих подій задається параметрами сигнатури атаки. Ці сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, число яких перевищує задані заздалегідь показники. Прикладом такої сигнатури є виявлення сканування портів або виявлення атаки SYN Flood. У першому випадку пороговим значенням є число портів, перевірених в одиницю часу. У другому випадку - число спроб встановлення віртуального з'єднання з вузлом за одиницю часу [6].

Як правило, сигнатури атак, створені на основі аналізу станів, описуються математичними моделями, що базуються на теорії кінцевих автоматів або мереж Петрі.

На рис. 2 показана мережа Петрі, що описує сигнатуру атаки, яка виконує підбір пароля для отримання несанкціонованого доступу до ресурсів ІС. Кожен перехід ІС в новий стан в цій мережі Петрі пов'язаний зі спробою введення пароля. Якщо користувач протягом 1 хв чотири рази поспіль введе неправильний пароль, то метод зафіксує факт здійснення атаки.

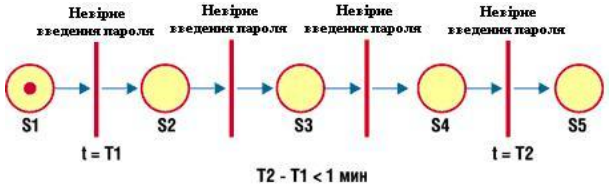

Рис. 2. Мережа Петрі, що описує сигнатуру атаки, яка здійснює підбір пароля.

Методи, що базуються на експертних системах, дозволяють описувати моделі атак на природній мові з високим рівнем абстракції. Експертна система, яку покладено в основу методів цього типу, складається з двох баз даних: фактів і правил. Факти це вихідні дані про роботу ІС, а правила - алгоритми логічних рішень про факт атаки на основі набору фактів. Всі правила експертної системи записуються в форматі "якщо <...>, то <...>". Результуюча база правил повинна описувати характерні ознаки атак, які зобов'язана виявляти СВВ.

Одна з найбільш перспективних сигнатурних груп - методи, які засновані на біологічних моделях. Для їх опису можуть використовуватися генетичні або нейромережеві алгоритми.

2.2 Метод виявлення аномалій або поведінковий метод. Поведінкові методи базуються не на моделях інформаційних атак, а на моделях штатного функціонування (поведінки) ІС. Принцип роботи будь-якого з таких методів полягає в виявленні невідповідності між поточним режимом роботи ІС і режимом роботи, що відповідає штатної моделі даного методу. Будь-яка невідповідність розглядається як інформаційна атака.

Наприклад, якщо система виявлення атак фіксує вхід співробітника компанії в мережу в суботу о 2.30, то це може свідчити про те, що пароль цього користувача вкрадений або підібраний і його зловмисник використовує для несанкціонованого проникнення [6].

Перевага методів даного типу - можливість виявлення нових атак без модифікації або поновлення параметрів моделі. На жаль, створити точну модель штатного режиму функціонування ІС дуже складно.

Серед поведінкових методів найбільш поширені ті, що базуються на статистичних моделях. Такі моделі визначають статистичні показники, що характеризують параметри штатної поведінки системи. Якщо з часом спостерігається певне відхилення даних параметрів від заданих значень, то фіксується факт виявлення атаки. Як правило, в якості таких параметрів можуть виступати рівень завантаження процесора, навантаження на канали зв'язку, штатний час роботи користувачів системи, кількість звернень до мережевих ресурсів і т. д.

Слід зазначити, що на стадії рекогносцировки, коли здійснюється збір інформації, ефективні лише сигнатурні методи виявлення атак. Справа в тому, що всі операції отримання необхідної порушнику інформації в більшості випадків не викликають ніякого відхилення роботи ІС від штатного режиму. Для цього етапу характерні такі ознаки, як формування запиту до DNS-сервера, отримання інформації з бази даних SNMP MIB або багаторазові TCP-запити на встановлення з'єднання з різними портами. На стадії рекогносцировки можуть використовуватися як мережеві, так і хостові датчики (табл. 1).

Таблиця 1

Застосування датчиків при виявленні вторгнень

Стадія атаки	Сигнатурний метод	Поведінковий метод
Рекогносцировка	+, СХ	-
Вторгнення в ІС	+, СХ	+, СХ
Атакуючий вплив	-	+, Х
Розвиток атаки	-	+, Х

Примітка: + - метод що може бути застосовано;
- - метод що може бути застосовано;
СХ - використовуються мережеві и хостові датчики;
Х - тільки хостові датчики

2.3. Застосовність сигнатурного і поведінкового методів для виявлення різних стадій атак. На стадії вторгнення виявити атаку можна за допо-

могою як сигнатурних, так і поведінкових методів. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у вигляді сигнатури, а з іншого - описати як якесь відхилення від штатної поведінки ІС. Найбільш ефективно поєднання обох методів, при цьому для отримання необхідних вихідних даних застосовні будь-які (хостові або мережеві) датчики.

Ефективне виявлення атак на етапах атакуючого впливу і розвитку атаки можливо тільки за допомогою поведінкових методів. Оскільки дії порушників залежать від цілей проведеної атаки і фіксованою безліччю сигнатур атак однозначно не визначаються. З огляду на той факт, що на двох останніх стадіях життєвого циклу інформаційної атаки найхарактерніші об'єкти - це хости, в даному випадку найбільш доцільно застосування хостових датчиків.

2.4. Недоліки існуючих систем виявлення. Недоліки сучасних СВВ можна класифікувати:

–пов'язані зі структурою СВВ;

–недоліки реалізації методів виявлення.

1. Аналіз структури СВВ дозволяє виділити такі їх властивості:

Відсутність загальної методології побудування - що можна пояснити недостатністю загальних угод в термінології, так як СВВ - це досить новий напрямок, заснований Андерсеном (J.P. Anderson) в 1980 році [8].

Ефективність. При використанні СВВ намагаються виявити будь-яку атаку, що призводить до суттєвого споживання ресурсів - для будь-якого профайла потрібні оновлення для кожного з спостережуваних подій.

Портативність. Більшість СВВ створюється для використання в певному програмно-апаратному середовищі, що призводить до ускладнення портування СВВ на інше програмно-апаратне середовище.

Оновлення. Складність поновлення СВВ виходить з прив'язки СВВ до програмно-апаратного комплексу та старіння однієї з частин цього комплексу обмежує застосування нових технологій для всієї системи.

Встановлення та налаштування СВВ. Для встановлення, налаштування і поновлення СВВ потрібно кваліфікований фахівець, що володіє спеціалізованими знаннями і навичками встановлення і налаштування експертної системи.

Продуктивність СВВ. Залежить від правил виявлення застосованих на кожному конкретному програмно-апаратному комплексі.

Відсутність загальних правил тестування.

2. *Аналізуючи реалізацію методів виявлення можно виділити наступні недоліки:*

– неприпустимо високий рівень помилкових спрацьовувань і пропусків атак;

– слабкі можливості по виявленню нових атак;

– на початкових етапах неможливо визначити більшість вторгнень;

– важко, іноді неможливо, визначити атакуючого, цілі атаки;

– відсутність оцінок точності і адекватності результатів роботи;

– неможливо визначати «старі» атаки, що використовують нові стратегії;

– складність виявлення вторгнень у реальному часі з необхідною повнотою в високошвидкісних мережах;

– слабкі можливості з автоматичного виявлення складних координованих атак;

– значне перевантаження систем, в яких функціонують СВВ, при роботі в реальному часі [9].

Складність застосування до СВВ формалізованого апарату аналізу та синтезу інформаційних систем полягає в тому, що конкретний інформаційний комплекс і його підсистема-СВВ складаються з різнорідних елементів, які можуть описуватися різними розділами теорії (системами масового обслуговування, кінцевими автоматами, теорією ймовірностей, теорією розпізнавання образів і т.д), тобто, даний об'єкт дослідження є агрегативним. Тому математичні моделі очевидно можна отримати тільки для окремих складових частин СВВ, що ускладнює аналіз і синтез СВВ в цілому, але подальша конкретизація застосування формалізованого апарату аналізу та синтезу дозволить оптимізувати СВВ [10].

Висновки

За результатами вище проведеного аналізу і із розрахунком перспективи подальшого впровадження перспективних технологій захисту інформації використання сигнатурного методу та методу виявлення аномалій забезпечують додатковий рівень захисту інформаційної системи, доповнюючи "традиційні" засоби захисту – міжмережеві екрани, криптомаршрутизатори, сервери аутентифікації та ін.

Чи можна виявити вторгнення в інформаційну систему? При всіх перерахованих недоліках дати ствердну відповідь можна. Найефективнішою СВВ можна вважати ту, яка працює в реальному часі і здійснює моніторинг трафіку мережі, а також відстежує аномалії, як в трафіку так і в діях користувачів і системи. Для ефективного виявлення атаки потрібно застосування як сигнатурного, так і поведінкового методів.

Найперспективнішим методом можна вважати комбінований метод, що використовує спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій. Так як, тільки комплексний підхід може значно знизити ризик вторгнення в ІС і виключити втрату цінних даних.

Для підвищення ймовірності виявлення атак на ІС потрібний збір великих обсягів інформації про функціонування ІС, а також їх аналіз.

Подальші напрямки вдосконалення пов'язані з усуненням недоліків сучасних СВВ: впровадження в практику апробованих теоретичних викладок з загальної теорії систем, методів теорії синтезу та аналізу інформаційних систем, конкретного апарату теорії розпізнавання образів. Але вони використовуються тільки для захисту комп'ютерів, а розповсюдженні платформи для мобільних пристроїв не мають такого захисту, що підвищує ризик зараження їх шкідливим програмним забезпеченням, приводячи до втрати інформації.

Як свідчать дані дослідження компанії Cisco кількість мобільних пристроїв з виходом в інтернет у 2016 році перевищило населення Землі [11].

Поточний стан справ із захистом даних, що зберігаються на мобільних пристроях в основному не відповідає вимогам безпеки обробки і зберігання даних. В якості прикладів локальних рішень можна назвати: антивіруси, утиліти шифрування та інші засоби, які ефективні самі по собі, але не призначені для організації комплексного централізованого захисту даних. Системи, що забезпечують такий захист, повинні надавати наступні можливості:

– дистанційне апаратне «скидання» пристрою;

– вибіркове або повне очищення пам'яті незалежно від місцезнаходження пристрою;

– контроль політик захищеності пристрою і даних;

– дистанційна доставка установок і оновлень;

– допомога користувачеві;

– багатоплатформенність.

Список літератури

1. Классификация угроз информационной безопасности [Електронний ресурс] Режим доступу: http://www.studfiles.ru/preview/6006132/page:2.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

3. Введение в информационную безопасность. Компьютеры: преступления, признаки уязвимости и меры защиты [Електронний ресурс] Режим доступу http://www.bezpeka.com/ru/lib/sec/gen/art344.html.

4. FAT [Електронний ресурс] Режим доступу https://ru.wikipedia.org/wiki/FAT.

5. Статистика мобильных операционных систем: популярность Android, первые проблемы Apple [Електронний ресурс] Режим доступу http://www.itrew.ru/windows/statistika-operacionnykh-sistem-za-ap.html.

6. Лукацкий А. Обнаружение атак. — СПб.: БХВ-Петербург, 2001. – 624 с.

7. Технологии обнаружения вторжений [Електронний ресурс] Режим доступу https://www.bytemag.ru/articles/detail.php?ID=6850&sphrase_id=3833171.

8. J.P. Anderson, Computer Security Threat Monitoring and Surveillance // James P. Anderson Co., Fort Washington, PA, April. 1980.

9. Городецкий В.И., Котенко И.В., Карсаев О.В., Хабаров А.В. Многоагентные технологии комплексной защиты информации в телекоммуникационных системах. ISINAS. 2000.

10. Бараматова И. С. Зайцева Е. В. Состояние и перспективы развития систем обнаружения компьютерных вторжений // Горный информационно-аналитический бюллетень (научно-технический журнал). Вып. S6. 2011

11. Кількість мобільних пристроїв з інтернетом скоро перевищить населення Землі [Електронний ресурс]. – Режим доступу: http://fmf.udpu.org.ua/novyny-suchasnoi-nauky/593-kilkist-mobilnykh-prystroiv-na-zemli-perevyshchyla-kilkist-liudei.

Надійшла до редколегії 24.03.2017

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський національний університет радіоелектроніки, Харків.

АНАЛИЗ И КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННУЮ СИСТЕМУ

В.В. Берковский, А.С. Бессонов

В статье анализируются угрозы и классифицирует методы обнаружения вторжений в информационную систему. Обнаружены недостатки, связанные со структурой СОВ и недостатки реализации методов выявления. Для повышения вероятности обнаружения атак на ИС наиболее перспективным будет использование комбинированного метода, а также создание унифицированной СОВ для защиты как компьютеров так и мобильных устройств. Определены дальнейшие направления совершенствования связанные с устранением недостатков современных СОВ. Использование сигнатурного метода и метода обнаружения аномалий обеспечивают дополнительный уровень защиты информационной системы, дополняя "традиционные" средства защиты для мобильных устройств.

***Ключевые слова**: системы обнаружения, системы вторжения, вторжения, сети, сигнатуры, системные аномалии, информационная атака.*

ANALYSIS AND CLASSIFICATION OF METHODS OF INTRUSION DETECTION IN THE INFORMATION SYSTEM

V.V. Berkovsky, A.S. Bessonov

The article analyzes the threats and klassificeret methods of intrusion detection in the information system. The deficiencies associated with the structure of SDI and disadvantages of the implementation of detection methods. To increase the likelihood of detection of attacks on IS is the most promising is the use of the combined method, as well as the creation of a unified SDI to protect both computers and mobile devices. Identify further areas of improvement related to elimination of faults in modern SDI. Using the signature method and the method of anomaly detection provides an extra level of protection of the information system, complementing "traditional" means of protection for mobile devices.

***Keywords:** system detection, system intrusion, intrusion, network, signature, system anomalies, information attack.*