5. Gonzalez, P. Pattern Recognition and Image Analysis [Text]/ First Iberian Conference, IbPRIA 2003: P. Gonzalez, Mallorca: Spain, 2003.- 1142p.
6. Annadurai, S. Digital Image Processing, 2/e [Text]/ S. Annadurai.-Addison-Wesley, 1993. – 716p.
7. Richardson, M. Fundamentals of Digital Image Processing [Text]/ M. Richardson.- Pearson Education India.- 2007. – 440p.
8. Kovalevskiĭ, V. A. Image pattern recognition [Text]/ V. A. Kovalevskiĭ.- .Springer-Verlag, 1980. – 241 p.
9. Tou, J. Pattern recognition principles [Text]/ J. Tou, R. Gonzalez.- Addison-Wesley Pub. Co., 1974. – 377p.
10. Jain, A. Fundamentals of digital image processing [Text]/ A. Jain.- Prentice Hall, 1989 – 569p.

В статі побудовано модель ризиків розповсюдження шкідливого програмного забезпечення (ШПЗ) та розкрито небезпеку електронним даним, пов'язану із впливом ШПЗ. Пропонується варіант концептуального підходу щодо протидії ШПЗ. Продемонстровано процес створення системи захисту організації від впливу ШПЗ

Ключові слова: ризик, безпека даних, кіберсередовище, шкідливе програмне забезпечення, вразливості, загрози, засоби захисту

В статье построена модель рисков распространения вредоносного программного обеспечения (ВПО) и раскрыта опасность электронным данным, связанная с влиянием ВПО. Предлагается вариант концептуального подхода по противодействию ВПО. Продемонстрирован процесс создания системы защиты организации от воздействия ВПО

Ключевые слова: риск, безопасность данных, киберсреда, вредоносное программное обеспечение, уязвимости, угрозы, средства зашиты

УДК 004.056

АНАЛІЗ РИЗИКІВ ВПЛИВУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БЕЗПЕКУ ДАНИХ В СУЧАСНОМУ КІБЕРСЕРЕДОВИЩІ

Ю. В. Копитін
Заступник начальника відділу забезпечення захисту інформації
Обласний інформаційно-аналітичний центр
Одеської обласної ради
пр-т Шевченка, 4, м. Одеса, Україна, 65032
E-mail: ykopitin@odessa.gov.ua

1. Вступ

В сучасному кіберсередовищі межі між інформаційно-комунікаційними технологіями, послугами та програмними застосуваннями стають все менш означеними, з більшою складністю та можливостями для обміну та передачі інформації, розвитку електронного урядування, ведення онлайн-бізнесу, надання мобільних та бездротових послуг [1]. Інформаційне (обчислювальне) та комунікаційне (мережеве) середовище є відкритим для все більшого числа ризиків і загроз, які можуть мати негативні наслідки для фізичних та юридичних осіб.

Розповсюдження шкідливого програмного забезпечення (ШПЗ) є однією з найбільш небезпечних загроз, що впливає на безпеку даних у сучасному кіберсередовищі. Дані, представлені в електронному вигляді, щодня піддаються небезпеці порушення конфіденційності, цілісності та доступності внаслідок впливу більш ніж 75 мільйонів різних примірників ШПЗ, що циркулює в інформаційно-комунікаційних системах та мережах [2].

2. Аналіз літературних даних та постановка проблеми

Дослідженню даної тематики відводиться значна увага міжнародних організацій (ITU, ISO, IETF), державних установ у багатьох країнах світу, виробників засобів захисту, провайдерів, організацій, а також вчених, зокрема, Пітера Грегорі, Камерон Малін, Косолапова Ф.А, Лукашева В.М., Молдовяна А.А., Мономахова Ю.М. та інших.

Однак, на сьогоднішній день відсутнє ризик-орієнтоване дослідження проблеми впливу шкідливого програмного забезпечення на кіберсередовище.

3. Мета та завдання дослідження

Мета дослідження – провести аналіз ризиків впливу ШПЗ на безпеку даних в сучасному кіберсередовищі та запропонувати ефективні заходи протидії його розповсюдженню.

Основними завданнями дослідження, спрямованими на досягнення поставленої мети, є:

- побудова моделі розповсюдження ШПЗ;
- формування концептуального підходу до забезпечення захисту кіберсередовища від впливу ШПЗ;
- розроблення процесу побудови ризик-орієнтованої системи захисту організації від ШПЗ.

4. Опис проблеми

Перш ніж перейти до опису проблеми, визначимо, що розуміється під шкідливим програмним забезпеченням (malware).

До шкідливого програмного забезпечення (шкідливого коду) відносяться програми, які впроваджуються в систему, як правило потай, з метою порушення конфіденційності, цілісності та доступності даних, програмного забезпечення або операційної системи жертви, або дратують чи дошкуляють жертві [3].

До такого програмного забезпечення відносяться віруси, хробаки, троянські програми, руткіти, шпіонське програмне забезпечення, рекламне програмне забезпечення, фальшиві антивіруси тощо.

Актуальність даної тематики пов'язана з тим фактом, що згідно із статистикою (рис. 1) [4] кількість примірників ШПЗ зростає по експотенційному закону.

За перше півріччя 2011 року в середньому щодня було виявлено 6881 новий примірник, що на 15,7% більше за минулий період.

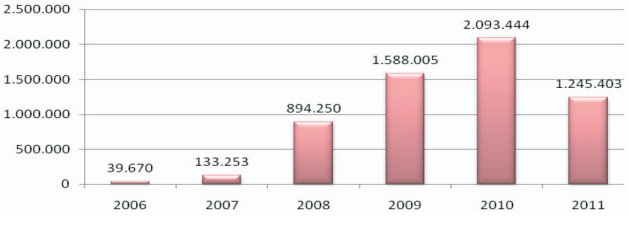

Рис. 1. Статистика появи шкідливого програмного забезпечення

При цьому жертвами кіберзлочинців стають, як іменити технологічні компанії, такі як Google, Sony, Lockheed Martin, PBS, Epsilon [5], так і звичайні користувачі, яких на сьогоднішній день переважна більшість. Зловмисники користуються тим, що простий користувач мало інформований про потенційні загрози Інтернету, та як наслідок здійснює типові помилки.

Незважаючи на зростання кількості та розширення різноманітності шляхів проникнення шкідливих кодів до комп'ютерних систем та мереж, мобільних засобів комунікацій, ефективної протидії ШПЗ до сих пір не створено [6].

Одним із основних стимулів швидкого зростання кількості примірників ШПЗ є грошова вигода. Причому значний прибуток зловмисниками отримується при низькому ризику ведення такої діяльності. В результаті циркуляції в кіберсередовищі ШПЗ формулюються додаткові складні фінансові потоки, які наведено у табл. 1 та представлено на рис. 2 [7]. Організації від впливу кіберзлочинності щорічно зазнають збитки у розмірі 114 млрд. доларів [8].

Таблиця 1

Фінансові потоки пов'язані з ШПЗ

Лінія на схемі (рис. 1)	Дія, яка відбувається
1	Фінансове вимагання, click-шахрайство, витрати пов'язані з викраденням ідентифікаційної інформації, фішинг
2	Не повернуті витрати, пов'язані з викраденням ідентифікаційної інформації, фішингом, брудними схемами та іншим електронним шахрайством
3, 4, 5, 6	Придбання обладнання зловмисниками, корпоративними та індивідуальними користувачами
7, 8, 9, 10	Замовлення послуг безпеки провайдерами, корпоративними та індивідуальними користувачами
11, 12, 13	Замовлення послуг провайдерів корпоративними та індивідуальними користувачами, зловмисниками
14	Виплати користувачам за збитки, пов'язані з крадіжкою ідентифікаційних даних

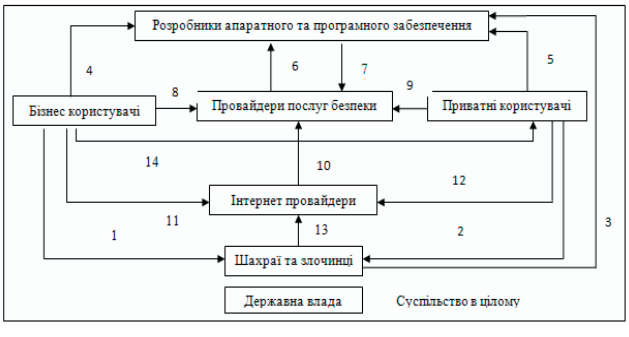

Рис. 2. Схема фінансових потоків пов'язаних з ШПЗ

Зазначимо, що дія ШПЗ спрямована не лише на системи, що містять інформацію з обмеженим доступом, а й на комп'ютери звичайних користувачів. Дана ситуація пов'язана з тим чинником, що в основній масі випадків зараження відбувається автоматизованим шляхом. В зв'язку з чим, необхідно забезпечувати захист від ШПЗ всіх електронних інформаційних активів.

Найчастіше зловмисники впроваджують ШПЗ у електронні ресурси, які користуються великою популярністю, а саме у: файлові обмінники, призначенні для розповсюдження піратського програмного забезпечення, соціальні мережі, гральні сайти, порно сайти.

Зазначимо, що послуги, пов'язані з розповсюдженням ШПЗ, можна легко замовити як через форуми чорного ринку, так і законними каналами продажу.

З іншого боку, актуальність побудови системи захисту від ШПЗ обумовлена величезною швидкістю розповсюдження ШПЗ. Так, мережевий хробак може швидко паралізувати роботу всіх комп'ютерів, що мають вихід до мережі Інтернет. Зазвичай для розповсюдження ШПЗ використовує вразливості наступних мережевих протоколів – HTTP, SMB, NetBIOS, SMTP, IRC, MSSQL, FTP, DCOM.

Одною з найбільш небезпечних кіберзагроз, сприяючих розповсюдженню ШПЗ, є експлойти нульово-

го дня, оскільки вони використовують помилки або вразливості у програмі чи операційній системі та з'являються відразу після виявлення даної уразливості, поки розробники програмного забезпечення ще не встигли створити патч, а адміністратори - вжити заходів безпеки [9].

На сьогоднішній день більшість з учасників інформаційного процесу не розуміють важливість впровадження заходів захисту від ШПЗ. На нашу думку однією з причин такої ситуації є відсутність чіткого стандарту з іменування ШПЗ [10]. В зв'язку з чим, в основній масі випадків під ШПЗ вважають виключно комп'ютерні віруси і для протидії йому достатньо встановити лише антивірусне програмне забезпечення, а не реалізувати цілий комплекс заходів захисту. Математичні моделі розповсюдження ШПЗ наведено в [11].

З метою підвищення рівня захищеності кіберсередовища від впливу ШПЗ побудовано графічну модель ризиків розповсюдження ШПЗ (рис. 3), на якій продемонстровано: найбільш розповсюджені типи ШПЗ та методи його розповсюдження, категорії розробників ШПЗ з зазначенням їх імовірної мети, причини впровадження ШПЗ та класичні заходи протидії розповсюдженню ШПЗ, порушувані властивості інформації та пов'язані з цим негативні наслідки.

Виходячи з описаної ситуації, на сьогоднішній день необхідно забезпечувати захист не лише від відомого ШПЗ, а й вміти блокувати нові невідомі до сьогоднішнього дня канали загроз.

5. Концептуальний підхід до забезпечення захисту кіберсередовища від шкідливого програмного забезпечення

Враховуючи майбутній потенціал он-лайн інформаційного суспільства, необхідно розробити чіткий концептуальний підхід щодо протидії розповсюдженню ШПЗ, яке є однією із основних кіберзагроз. При цьому безпека інформаційних систем та мереж повинна розглядатися не лише з точки зору технологій, а також враховувати такі елементи, як попередження ризиків, управління ризиками та підвищення поінформованості користувачів.

Концептуальний підхід надасть змогу на міжнародному рівні уніфікувати методи боротьби з ШПЗ та враховувати всі стратегічні принципи, а саме: правові, технічні та процедурні заходи, організаційну структуру, створення потенціалу та міжнародне співробітництво [12].

Тобто він має виступити в якості шаблону, яким будуть керуватися органи державної влади, а також юридичні та фізичні особи. Нижче спробуємо надати варіант концептуального підходу, який дозволить уникнути помилок, пов'язаних з побудовою системи захисту власними силами.

Захист кіберсередовища від ШПЗ є загальним обов'язком, який може бути найкращим чином реалізований за допомогою співробітництва між органами державної влади (ОДВ) на всіх рівнях та приватним сектором, який володіє значною частиною інформаційної інфраструктури та експлуатує її.

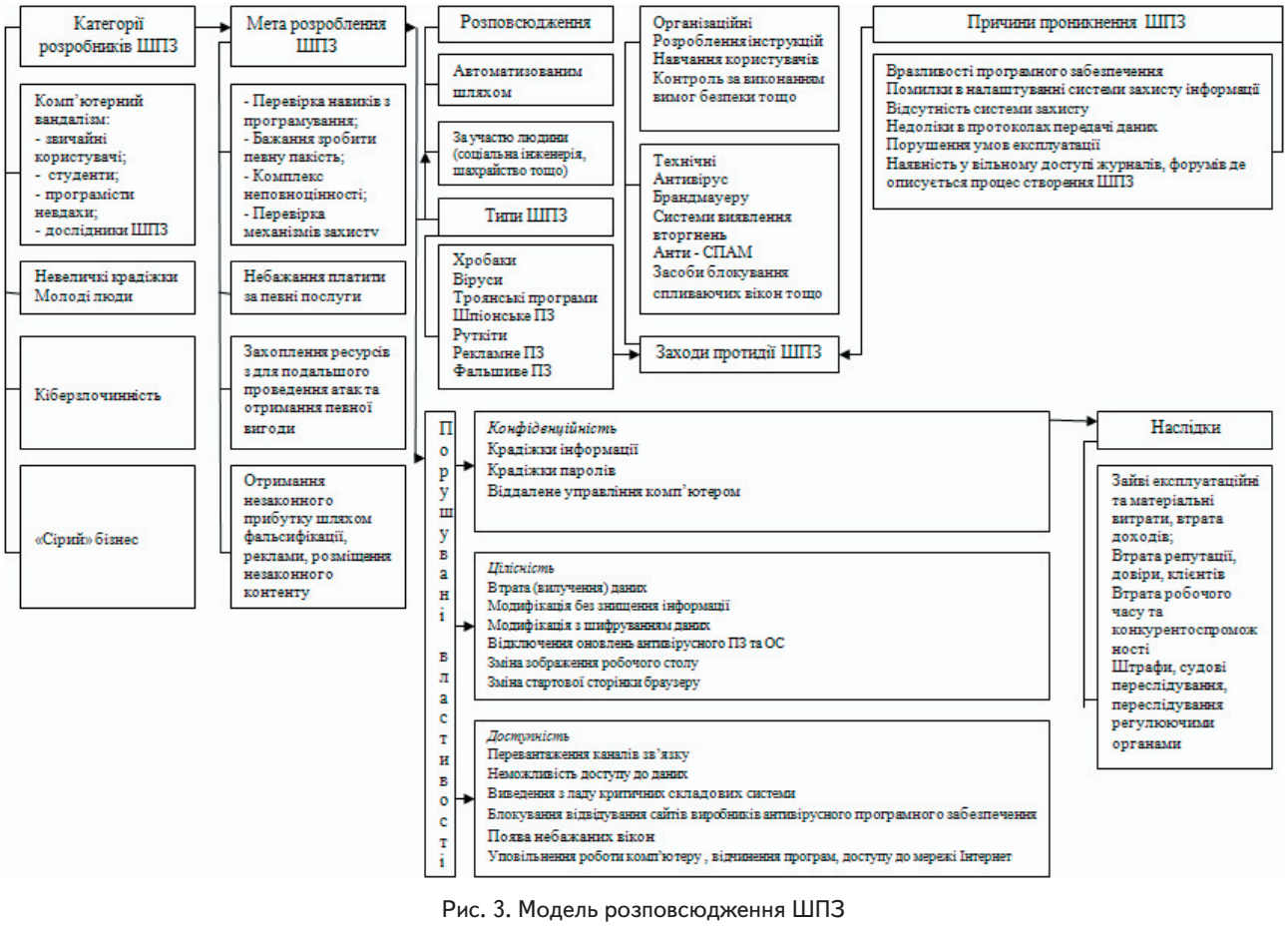

Рис. 3. Модель розповсюдження ШПЗ

ОДВ при цьому повинні розробляти інформаційну політику з урахуванням вимог кібербезпеки та забезпечувати контроль за її виконанням [13].

Також для підвищення стійкості та надійності системи захисту від ШПЗ важливо забезпечити співпрацю між власниками систем та операторами мереж зв'язку.

Для реалізації ефективної співпраці потрібно забезпечити наявність трьох важливих елементів: повної демонстрації переваг; чіткого розмежування функцій і обов'язків кожної із сторін; взаємної довіри.

Основними перевагами для держави є те, що приватний сектор володіє можливостями, які зазвичай виходять за межі органів влади, наприклад:

- володіння і управління більшою частиною інформаційної інфраструктури;
- знання ресурсів, мереж, систем, засобів, функцій та інших можливостей;
- досвід реагування на інциденти;
- впровадження нововведень і надання продуктів, послуг і технологій для швидкого задоволення потреб суспільства;
- проектування, розгортання, експлуатація, управління та обслуговування мережі Інтернет.

Основними перевагами для приватного сектору у взаємодії з ОДВ є те, що вони можуть:

- надавати власникам і операторам своєчасну, аналітичну, достовірну, узагальнену та корисну інформацію про загрози;
- залучати приватний сектор до розробки ініціатив та політик інформаційної інфраструктури;
- роз'яснювати керівникам корпорацій, використовуючи відкриті платформи та пряме спілкування, вигоди, як для комерційних підприємств, так і для національної безпеки, інвестування в заходи щодо забезпечення безпеки, що виходять за рамки їх конкретних ділових стратегій;
- співпрацювати з приватним сектором з метою формулювання та чіткого визначення пріоритетів щодо основних функцій та забезпечення їх захисту та/або відновлення тощо.

Даний підхід передбачає чіткий розподіл повноважень між органами державної влади, міжнародними організаціями з стандартизації, провайдерами, виробниками програмно-апаратного забезпечення, кінцевими споживачами послуг.

Для покращення рівня захищеності від ШПЗ міжнародним організаціям необхідно виробити єдині вимоги щодо забезпечення захисту від ШПЗ, які включатимуть:

- чітку класифікацію ШПЗ, що допоможе уніфікувати діяльність пов'язану з боротьбою з ним;
- обов'язкове впровадження захисних механізмів у свої продукти виробниками апаратного та програмного забезпечення;
- налаштування та технічну підтримку програмного забезпечення, призначеного для захисту інформації, його виробниками. Захисне програмне забезпечення повинно виступати в якості послуги, яку користувачі періодично замовлятимуть;
- встановлення засобів антивірусного та мережевого захисту, протидії СПАМу операторами (провайдерами) послуг зв'язку;
- обов'язкове створення команд реагування на інциденти інформаційної безпеки на рівні держави, провайдерів, організацій;
- розроблення рекомендацій провайдерами та виробниками програмного забезпечення щодо безпечної роботи за комп'ютером у мережі Інтернет, з системою електронної пошти та іншими послугами кінцевим споживачам (звичайним користувачам).

На рівні органів державної влади необхідно забезпечити:

- розроблення законодавчих вимог щодо організації процесу захисту від ШПЗ, координації діяльності всіх установ, міжнародної взаємодії, а також посилення всіх видів відповідальності за навмисне виробництво та збут ШПЗ;
- залучення до розроблення рекомендацій щодо захисту від ШПЗ приватних установ, оскільки саме вони в основному і є власниками більшості з мереж та систем;
- координацію взаємодії між національною командою реагування на інциденти інформаційної безпеки та командами реагування провайдерів та інших приватних установ;
- організацію науково-практичних досліджень з питань розроблення та вдосконалення механізмів протидії розповсюдженню ШПЗ, а також підтримку проведення форумів, конференцій, семінарів тощо.

Для ефективної реалізації даної концепції, кінцевим споживачам необхідно буде лишу чітко дотримуватися рекомендацій, які будуть розроблені на державному рівні, провайдерами та виробниками програмного забезпечення.

Такий підхід дозволить забезпечити надійний захист більшості звичайних користувачів, які не володіють жодними навиками безпеки при роботі в мережі Інтернет, та ряду організацій, які не можуть забезпечити захист власними силами.

Для якісної реалізації рекомендованих заходів, всі учасники процесу боротьби з ШПЗ повинні надавати виключно правдиву інформацію щодо появи нових загроз та пов'язаних з ними ризиками, заходів протидії, чітко виконувати наведені рекомендації та гарантувати не перекручування інформації.

6. Процес побудови системи захисту організації від ШПЗ

Враховуючи вимоги міжнародного стандарту ISO 27005:2011 [14], рекомендацій ITU-T X.1207 [15] та стандарту NIST 800-83 [3] процес побудови системи захисту організації від ШПЗ можна поділити на 4 етапи: оцінка ризиків розповсюдження ШПЗ; вибір та впровадження заходів щодо обробки ризиків розповсюдження ШПЗ; обмін інформацією про ризики; моніторинг рівня ризику розповсюдження ШПЗ.

Оцінка ризиків розповсюдження ШПЗ включає:

- визначення та класифікацію активів, що впливають на імовірність зараження ШПЗ. На даному кроці необхідно визначити активи, які найбільше впливають на імовірність зараження ШПЗ, а саме: апаратно-програмне забезпечення, яке використовується в роботі, користувачів інформаційної системи, а також робочі цілі та імідж організації;

- ідентифікацію використовуваних в поточний момент заходів захисту від ШПЗ. Для подальшого моделювання та аналізу сценаріїв реалізації загрози зараження системи або мережі ШПЗ необхідно ідентифікувати всі використовувані засоби та заходи захисту. Основні заходи описано на етапі, що стосується вибору та впровадження заходів щодо обробки ризиків розповсюдження ШПЗ;

- аналіз імовірних сценаріїв реалізації загрози зараження ШПЗ. Виходячи з попередньо ідентифікованих активів та заходів безпеки, для подальшого вибору актуальних механізмів безпеки, необхідно побудувати модель імовірних сценаріїв проникнення ШПЗ до системи або мережі.

Вибір та впровадження заходів щодо обробки ризиків розповсюдження ШПЗ включає вибір та впровадження організаційних та технічних заходів захисту, спрямованих на зниження імовірності реалізації загроз та зменшення наслідків від реалізації загроз. До організаційних заходів, спрямованих на зниження імовірності реалізації загроз, відносяться:

1. Розподіл обов'язків між співробітниками організації щодо організації та забезпечення захисту від ШПЗ, а саме:

- визначення підрозділу, який буде організовувати роботу з забезпечення захисту від ШПЗ, або відповідальну особу;

- покладення відповідальності за виконання вимог щодо захисту від ШПЗ у структурних підрозділах організації на керівників підрозділів, а обов'язків щодо виконання установлених заходів захисту від ШПЗ - на кожного користувача (співробітника);

- документальне закріплення обов'язків та відповідальності користувачів щодо виконання вимог з протидії ШПЗ.

2. Проведення навчання та атестації всіх користувачів щодо знання правил захисту від розповсюдження ШПЗ.

3. Забезпечення чіткого контролю за виконанням користувачами вимог безпеки підрозділом відповідальним за захист від ШПЗ.

4. Проведення постійного аналізу ефективності та достатності вжитих заходів та засобів захисту від впливу ШПЗ.

5. Визначення та документальне закріплення дозволеного програмного забезпечення, необхідного для виконання посадових обов'язків.

До організаційно-технічних заходів щодо зниження імовірності реалізації загроз відносяться:

1. Забезпечення підрозділом відповідальним за захист від ШПЗ:

- встановлення останніх оновлень операційної системи та прикладного програмного забезпечення;

- проведення періодичного сканування на наявність зайвих відчинених портів на серверах та робочих станціях;

- організації щоденного сканування серверів та найбільш критичних ресурсів системи;

- унеможливлення підключення стороннього обладнання (точки доступу, модеми, маршрутизатори тощо);

- проведення щотижневого повного сканування комп'ютерів на пошук ШПЗ;

- відключення автозавантаження змінних носіїв на комп'ютерах;

- створення точок відновлювання операційної системи;

- встановлення паролю на адміністративний обліковий запис в операційній системі, відомий лише співробітникам підрозділу забезпечення захисту від ШПЗ, який необхідно використовувати виключно для налаштування операційної системи, інсталяції програмного забезпечення та інших адміністративних задач;

- регулярного очищення куків браузерів;

- моніторингу коректності функціонування засобів захисту від ШПЗ;

- контролю за виконанням усіма користувачами заходів захисту від ШПЗ.

2. Всім користувачам необхідно:

- працювати під обліковим записом з обмеженими правами та захищеним паролем;

- перевіряти антивірусним програмним забезпеченням (АПЗ) перед кожним використанням всі змінні носії інформації;

- перевіряти АПЗ всі файли, отримані електронною поштою, програмами миттєвого обміну повідомленнями або завантажені з мережі Інтернет;

- звертати особливу увагу на адресу відправника поштової кореспонденції при роботі з електронною поштою. Якщо відправник поштового повідомлення невідомий – відкривати вкладення з такого листа категорично не рекомендується;

- проводити резервне копіювання даних, що зберігаються на комп'ютері.

До технічних заходів щодо зниження імовірності реалізації загроз відноситься встановлення:

- мережевого брандмауеру;

- мережевої системи виявлення вторгнень;

- АПЗ на рівні шлюзів, систем електронної пошти, файлових серверів;

- програмного забезпечення для захисту від СПАМу;

- програмних засобів, призначених для захисту комп'ютеру від ШПЗ (антивірус, анти-шпигун);

- засобів, які забезпечують блокування спливаючих вікон у браузері та запуск активних скриптів;

- локальної системи виявлення та попередження вторгнень (HIPDS);

- персонального брандмауеру.

До організаційних заходів зменшення наслідків реалізації загроз відносяться:

1. Створення команди реагування на інциденти інформаційної безпеки.

2. Розроблення документації, яка регламентуватиме порядок обробки інцидентів, пов'язаних з впливом ШПЗ, а також журналів, в які будуть заноситися відомості про інциденти безпеки.

3. Ознайомлення користувачів з правилами поведінки у випадку підозри на зараження комп'ютеру ШПЗ.

4. Придбання полюсу страхування від впливу ризиків інформаційної безпеки пов'язаних з пошкодженням даних внаслідок впливу ШПЗ.

До організаційно-технічних заходів зменшення наслідків реалізації загроз відносяться:

- формування переліку засобів щодо виявлення та аналізу інцидентів, пов'язаних з впливом ШПЗ. Для його формування можна скористатися рекомендаціями наведеними в [16];

- забезпечення реєстрації та збереження інформації про події інформаційної безпеки.

Обмін інформацією про ризики передбачає розподіл думок між особою, яка приймає рішення, пов'язані з визначенням його рівня та іншими зацікавленими сторонами.

Сприйняття ризику може змінитися через відмінності в припущеннях, поняттях і потребах різних сторін, тобто можуть з'явитися різні погляди. Даний обмін інформацією важливий для досягнення:

- вибору оптимальних варіантів оброблення ризиків;

- зменшення наслідків від розповсюдження ШПЗ через брак взаємного розуміння серед осіб, що приймають керівні рішення та іншими сторонами;

- підтримки прийняття рішення;

- доведення відповідальності про ризики особам, які приймають керівні рішення та іншим сторонам.

Моніторинг рівню ризику розповсюдження ШПЗ передбачає перевірку та перегляд ризиків та їх чинників з метою своєчасного виявлення будь-яких змін, що можуть вплинути на рівень захищеності.

Організації необхідно регулярно перевіряти наступне:

- появу нових активів, що можуть вплинути на рівень захищеності;

- виникнення нових загроз, які не були оцінені раніше, і, можливо, активні як всередині, так і зовні організації;

- збільшення наслідків або імовірності реалізації загроз;

- виникнення інцидентів інформаційної безпеки.

Таким чином, враховуючи обсяг описаних вище заходів з протидії розповсюдженню ШПЗ, необхідно провести додаткові дослідження вразливостей систем та мереж на всіх фазах життєвого циклу (проектування, створення, монтаж, модернізація, експлуатація, списання або заміна окремих компонентів) та схем інформаційних потоків, з точки зору визначення максимально можливої кількості каналів розповсюдження ШПЗ.

7. Висновки

Проведений в роботі аналіз ризиків впливу ШПЗ на безпеку даних в сучасному кіберсередовищі показав, що дана загроза є однією з найнебезпечніших та може швидко паралізувати роботу всіх комп'ютерів, що мають вихід до мережі Інтернет. Використання побудованої графічної моделі та процесу впровадження заходів захисту від ШПЗ, дозволить організаціям зрозуміти масштаби проблеми та вибрати оптимальні рішення щодо забезпечення захисту конфіденційності, цілісності та доступності електронної інформації.

Запропонований варіант концепції захисту від ШПЗ дозволить підвищити рівень захищеності даних на глобальному рівні шляхом координації зусиль органів державної влади та приватного сектору.

Література

1. ITU-T X.1055. Risk management and risk profile guidelines for telecommunication organizations [Текст]. – Введ. 2008-11-13. – Женева, 2008 . – 22 с.
2. McAfee Threats Report: Second Quarter 2011 [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q2-2011.pdf - 2011 р.
3. NIST Special Publication 800-83. Guide to Malware Incident Prevention and Handling [Текст]. – Gaithersburg, 2005 . – 101 с.
4. G-Data Malware Report. Half-yearly report January [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.gdatasoftware.com/uploads/media/G_Data_MalwareReport_H1_2011_EN.pdf - 2011 р.
5. Сделать онлайновый мир безопаснее [Електронний ресурс]. – Режим доступу: \www/ URL: https://itunews.itu.int/Ru/Note.aspx?Note=1484 – 2011 . – Загол. з екрану.
6. Современная антивирусная индустрия и её проблемы [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.securelist.com/ru/analysis?pubid=174261388– 2011 . – Загол. з екрану.
7. Malware risks and mitigation report [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf - 2011 р.
8. Убытки от киберпреступности в мире ежегодно составляют 114 миллиардов долларов [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.e-moneynews.ru/ubytki-ot-kiberprestupnosti-114-milliardov - 23.09.2011 р. – Загол. з екрану.
9. Zero-day эксплойт [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.securelist.com/ru/glossary?glossid=-152528354. – Загол. з екрану.
10. Классификация детектируемых объектов [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.securelist.com/ru/threats/detect?chapter=32 . – Загол. з екрану.
11. Монахов, Ю.М. Вредоносные программы в компьютерных сетях : учеб. пособие / Ю.М. Монахов, Л.М. Груздева, М.Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2010. – 72 с. (Комплексная защита объектов информатизации. Кн. 19). – ISBN 978-5-9984-0087-2.
12. The 2011 (ISC)2 Global Information Security Workforce Study [Електронний ресурс]. – Режим доступу: \www/ URL: https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf - 2011 р.

13. QUESTION 22/1: Securing information and communication networks: best practices for developing a culture of cybersecurity [Електронний ресурс] / International Telecommunication Union. – Режим доступу: \www/ URL: http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf - 2010 p.
14. ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management (second edition) [Текст]. – Введ. 2011-05-19. – Женева, 2011. – 68 с.
15. ITU-T X.1207. Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software [Текст]. – Введ. 2008-04-18. – Женева, 2008 . – 20 с.
16. Cameron H. Malin Malware Forensics: Investigating and Analyzing Malicious Code [Текст]:/ Cameron H. Malin, Eoghan Casey, James M. Aquilina. – 1 edition. – Waltham: Syngress, 2008. – 592 с.

Ми розглядаємо методи та засоби Business Intelligence для аналізу фінансових показників банку, наводимо доцільність використання експертної системи у галузі Business Intelligence, і на основі цього проводимо дослідження процесу індустріального тестування експертних систем. Розглядаємо аналітичний додаток аналізу фінансових показників банку з використанням методів та засобів BI. Детально розглядаємо реалізацію OLAP рішення

Ключові слова: Business Intelligence, Reports Services, тестирование, метрики, экспертные системы, искусственный интеллект

Мы рассматриваем методы и средства BI для анализа финансовых показателей банка, приводим целесообразность использования экспертной системы в сфере BI, и на основе этого проводим исследование процесса индустриального тестирования экспертных систем. Рассматриваем аналитическое приложение анализа финансовых показателей банка с использованием методов и средств BI. Подробно рассматриваем реализацию OLAP решения

Ключові слова: Business Intelligence, Reports Services, тестування, метрики, експертні системи, штучний інтелект

УДК 004.89

ПРОЦЕСИ ТЕСТУВАННЯ ЕКСПЕРТНИХ СИСТЕМ ДЛЯ ВПРОВАДЖЕННЯ В BUSINESS INTELLIGENCE

Н.В. Ковтун*
E-mail: natalivalentain@gmail.com
М.М. Нестеренко*
E-mail: misha.nesterenko@gmail.com
І. В. Цемкало*
E-mail: irina.tsemkalo@gmail.com
*Кафедра програмної інженерії
Харківський національний університет радіоелектроніки
пр. Леніна, 14, м. Харків, Україна, 61166

1. Вступ

Підвищення прибутковості, зниження собівартості, розширення ринків збуту підприємств неможливе без аналізу бізнес-процесів. Як правило, бізнес-аналіз необхідний на всіх стадіях життєвого циклу продукту й у всіх підрозділах підприємства, це в свою чергу потребує обробки величезних обсягів інформації. Бізнес-аналітики великих IT компаній займаються структуруванням інформації, написанням інтерфейсів доступу до неї, забезпеченням безпеки, цілісності та інших проблем, пов'язаних з аналізом. Існують зручні і гнучкі засоби, що дозволяють відобразити потрібні розрізи цієї інформації, що дозволяє управлінцям і аналітикам приймати оптимальні рішення для поліпшення всіх показників функціонування.

Найбільш цікавим питанням є інтеграція засобів BI з можливостями експертних систем. Експертні системи розроблюються як практичне використання досліджень у галузі штучного інтелекту (ШІ). Вони комбінують знання про деяку галузь діяльності людини з можливістю робити висновки, які засновані на відомих фактах та правилах застосування знань до відомих фактів. При наявності високоякісних знань (які добре відображають реальність) продуктивність експертної системи може наблизитись до продуктивності людини-експерта, а в деяких випадках навіть перевершити продуктивність людини. Експертні системи з'явились як допоміжні програмні додатки у галузях медичного діагностування, розшуку мінералів та автоматизованого налаштування програмних систем. На даний момент вони все глиб-