УДК 004.056, 681.513.5:623.4 **Бурячок В.Л.**

АЛГОРИТМ ОЦІНЮВАННЯ СТУПЕНЯ ЗАХИЩЕНОСТІ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

У статті викладений можливий варіант механізму оцінювання ступеня захищеності спеціальних ІТС з точки зору дій системного адміністратора та дій, що виконуються системою аналізу ступеня захищеності системи. Окрім цього досліджені проблемні питання оцінювання загроз безпеці інформації в СІТС за метою реалізації з позицій забезпечення її конфіденційності, цілісності і доступності.

Ключові слова: алгоритм, інформаційне суспільство, інформаційно-комунікаційна технологія, інформаційно-телекомунікаційна система, кібербезпека, кіберзлочин, кіберпростір, кіберзагроза, загроза конфіденційності, загроза цілісності, загроза доступності

Постановка завдання у загальному вигляді. Науково-технічна революція наприкінці XX початку XXI сторіччя викликала у світі глибокі системні перетворення. Вони, як результат, дали можливість завдяки синтезу перспективних інформаційно-комунікаційних технологій (далі, ІКТ) і бурхливого розвитку електронної обчислювальної техніки (далі, ЕОТ) сформуватись та розвинутись принципово новим і невід'ємним глобальним субстанціям: інформаційному суспільству, інформаційному простору та його окремій складовій – простору кібернетичному (далі, кіберпростір). Нині всі вони мають практично необмежений потенціал і відіграють суттєву роль в економічному та соціальному розвитку будь-якої країни світу. Системорганізуючою основою, матеріальною і технологічною базою цих субстанцій стали віртуальний і реальний простори, утворені за допомогою сучасних інформаційно-телекомунікаційних систем (далі, ІТС) загального та спеціального призначення, мережних технологій цивільного та/або військового спрямування, програмних засобів і засобів зв'язку, без яких в умовах сьогодення неможливо забезпечити обробку і передачу їх головного об'єкта – інформації.

Неконтрольоване поширення і використання віртуального та реального просторів, перш за все як сфери ведення воєнних конфліктів сучасності і найближчого майбутнього, зростання впливу засобів масової інформації (далі, ЗМІ), а також впливу ІКТ та ІТС на постіндустріальне суспільство, поява небезпеки розриву між інформаційною елітою та споживачами призвело, у свою чергу, до того, що поряд з отриманням значних переваг від застосування інформаційного та кіберпросторів світове співтовариство набуло й усі пов'язані з ними проблеми. Внаслідок чого суттєво ускладнилось завдання добування даних, що необхідні органам державного та військового управління для прийняття виважених, адекватних умовам обстановки рішень, а також їх захисту від різного роду деструктивних впливів – викликів, фактично неприхованих кібернетичних злочинів і загроз.

Аналіз останніх досліджень і публікацій. Цю проблему висвітлено в багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи Возженікова А.В., Ліпкан В.А., С.В. Ленкова, Мірошниченко В.М., Хорошка В.О., Ярочкіна В.І., Мініхена К.А., М. Лібіцкі, О. Шермана та інших фахівців. Тим не менш аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексне дослідження проблеми, перш за все інформаційної та кібернетичної безпеки, методів, які при цьому застосовуються, а також їх особливостей на цей час практично відсутнє. Тому, враховуючи реалії сьогодення, вона потребує додаткового і більш глибокого вивчення.

Актуальність та мета статті. Все це фактично дає можливість стверджувати, що проблеми інформаційної та кібернетичної безпеки за сучасних умов і для України, і для переважної більшості інших держав світу стають нині особливо актуальними. Відповідно, метою статті є формування зрозумілого, науково-обґрунтованого понятійного апарату в цій предметній області, а також алгоритму оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем (далі, СІТС) у інформаційному і кібернетичному просторах.

Виклад основного матеріалу. Під **СІТС** згідно [1, 2] будемо розуміти сукупність інформаційних та телекомунікаційних систем, що складаються з ряду взаємозалежних функціональних елементів – підсистем та їх окремих компонент, орієнтованих на виконання визначених функцій і завдань та які у процесі обробки інформації діють як єдине ціле. Мета їх створення, як відомо [1, 2], полягає в тому, щоб у гранично короткі терміни створити систему обробки даних, яка має задані споживчі якості, а саме: продуктивність, відмовостійкість, сумісність, розширюваність, масштабованість та ефективність, а також забезпечити інформаційну і кібернетичну безпеку цих даних.

В цьому випадку під **інформаційною та кібернетичною безпекою СІТС** згідно [3-6] будемо розуміти, відповідно, здатність цих систем:

1. Протистояти спробам випадкового або навмисного деструктивного впливу (проникнення) природного або штучного характеру в нормальний процес їх функціонування на різних етапах життєвого циклу, а також розкрадання, модифікації або руйнування циркулюючої в них інформації;

2. Забезпечити своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних, фактично неприхованих викликів, кібернетичних злочинів і загроз.

З урахуванням викладеного та положень [7] алгоритм аналізу ступеня захищеності СІТС від різноманітних викликів, кібернетичних злочинів і загроз або інакше алгоритм аналізу ступеня забезпечення їх інформаційної та кібербезпеки може бути поданий у спосіб, що представлений на рис. 1.

В рамках комплексного розгляду питань забезпечення інформаційної безпеки СІТС дії у межах алгоритму умовно розділені на дві групи: дії системного адміністратора та дії, що виконуються системою аналізу ступеня захищеності. При цьому особлива увага в ході його практичної реалізації має бути приділена загрозам безпеки, службам безпеки й механізмам реалізації функцій служб безпеки.

Під **загрозами безпеки** у даному випадку будемо розуміти події, які шляхом потенційно можливого впливу на СІТС прямо та/або опосередковано завдають збитку її власникам і користувачам. Вони можуть бути класифіковані за такими основними ознаками (рис. 2): за метою реалізації, за джерелами, за засобами, за методами і наслідками, а також за принципами, характером та способами впливу на певний об'єкт.

Загрози безпеці інформації в СІТС за метою реалізації представляють собою найбільший інтерес з позицій класифікації кібернетичних злочинів і загроз за схемою, пропонованою Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю. Вони полягають у порушенні: конфіденційності інформації (властивість інформації бути відомою в плані читання або копіювання тільки допущеним або інакше авторизованим суб'єктам СІТС: користувачам, програмам, процесам); цілісності інформації (властивість інформації бути незмінною в семантичному змісті, що досягається сукупністю заходів щодо її захисту від збоїв, видалення і несанкціонованого доступу до неї); працездатності СІТС та/або доступності до інформації, що в ній циркулює (властивість інформації бути захищеною від несанкціонованого блокування), у будь-який час для всіх авторизованих користувачів, - й реалізуються порушниками через несанкціонований доступ в інформаційне середовище, незаконне втручання в дані та/або їх перехоплення, незаконне використання комп'ютерного й телекомунікаційного встаткування або його повне вилучення тощо.

При цьому **до загроз порушення конфіденційності інформації в СІТС** згідно з [8, 9] належать, як правило, спроби несанкціонованого: читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що відносяться до різних класів захищеності тощо. З урахуванням положень [10], вони ймовірно можуть бути реалізовані неавторизованим користувачем (порушником) за умови подолання ним засобів: організаційного обмеження доступу (p_{ood}); охоронної сигналізації (p_{oc}); захисту від вірусних атак ($p_{атак}$); канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ

($p_{кзткм}$); управління доступу, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{уфд}$), а також адміністрування доступу до відповідних суб'єктів і об'єктів з використанням механізмів загального і спеціального ПЗ ($p_{ад}$).Виходячи з такого ймовірність подолання неавторизованим користувачем зазначених засобів захисту може бути визначена з виразу:

$$p_{пзз} = p_{уфд} \cdot p_{ад} \cdot \left[1 - \left(1 - p_{ооД}\right) \cdot \left(1 - p_{ос}\right) \cdot \left(1 - p_{атак}\right) \cdot \left(1 - p_{кзктм}\right)\right]. \quad (1)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за умови, якщо порушник після її отримання: знає мову, якою інформація представляється (ймовірність події - $p_{мова}$); знає і може застосовувати програмні засоби або апаратуру криптографічного перетворення (ймовірність події - $p_{пз/ктп}$); має необхідні ключі або ключові набори для такого перетворення (ймовірність події - $p_{ключі}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем засобів криптографічного захисту з урахуванням положень [10] може бути визначена з виразу:

$$p_{êç^3} = p_{ì\,î\,âà} \cdot p_{ï\,ç/êò\,ï} \cdot p_{êëp\,\div^3}. \quad (2)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих вище засобів може бути визначена як:

$$P_{ПКІ} = p_{кзі} \cdot \left[1 - \left(1 - p_{пзз}\right)\right]. \quad (3)$$

До загроз порушення цілісності інформації в СІТС, як відомо [8, 9], належать: несанкціонована модифікація та/або видалення програм і даних; вставка, зміна або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі; втрата даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо. Вони ймовірно можуть бути реалізовані неавторизованим користувачем за умови подолання ним засобів: організаційного обмеження доступу, охоронної сигналізації та управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо та адміністрування доступу, як й при аналізі загроз конфіденційності інформації (ймовірність такої події - $p_{пзз}$ визначена раніше); захисту цілісності від загроз у телекомунікаційних мережах ($p_{цткм}$); захисту від спеціальних впливів на інформацію по ТКМ ($p_{сп.вп}$); контролю та поновлення цілісності інформації ($p_{конт.ц}$).

З урахуванням можливостей попереднього підходу, ймовірність порушення цілісності $P_{ПЦІ}$ може бути знайдена з виразу:

$$P_{ПЦІ} = p_{конт.ц} \cdot \left[1 - \left(1 - p_{пзз}\right) \cdot \left(1 - p_{сп.вп}\right) \cdot \left(1 - p_{цткм}\right)\right]. \quad (4)$$

До загроз порушення доступності інформації в СІТС згідно з [8, 9] відноситься: повторення або вповільнення елементів протоколу; придушення обміну в телекомунікаційних мережах; використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні; перевитрата обчислювальних або телекомунікаційних ресурсів тощо. Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до інформаційних ресурсів ЛОМ (ідентифікації, автентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації.

Виходячи з такого стійкість системи управління доступом - (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{пзз}. \tag{5}$$

Ця задача може вирішуватися застосуванням у СІТС засобів фільтрації типу міжмережних екранів (*firewall*, брандмауерів), сервісів-посередників (*proxyservices*) тощо. При середній тривалості обслуговування в СІТС одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, згідно [10] дорівнює:

$$p_{вик.рес} = 1 - p_0 = 1 - \exp\{- t_{вик.рес} \cdot \lambda_{зап}\}, \tag{6}$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів); $t_{вик.рес}$ – середнє значення часу використання ресурсу.

Враховуючи таке ймовірність порушення доступності ресурсу з урахуванням положень [10] дорівнюватиме:

$$P_{ПДІ} = 1 - (1 - p_{вик.рес}) \cdot (1 - p_{ссуд}). \tag{7}$$

Виходячи з наведених вище формульних залежностей комплексна величина ймовірності порушення системи захисту інформації у СІТС та їх специфічному класі – ЛОМ за метою реалізації з урахуванням пропозицій [10] може бути, як результат, знайдена з виразу:

$$P_{ПСЗІ} = 1 - (1 - P_{ПКІ}) \cdot (1 - P_{ПЦІ}) \cdot (1 - P_{ПДІ}). \tag{8}$$

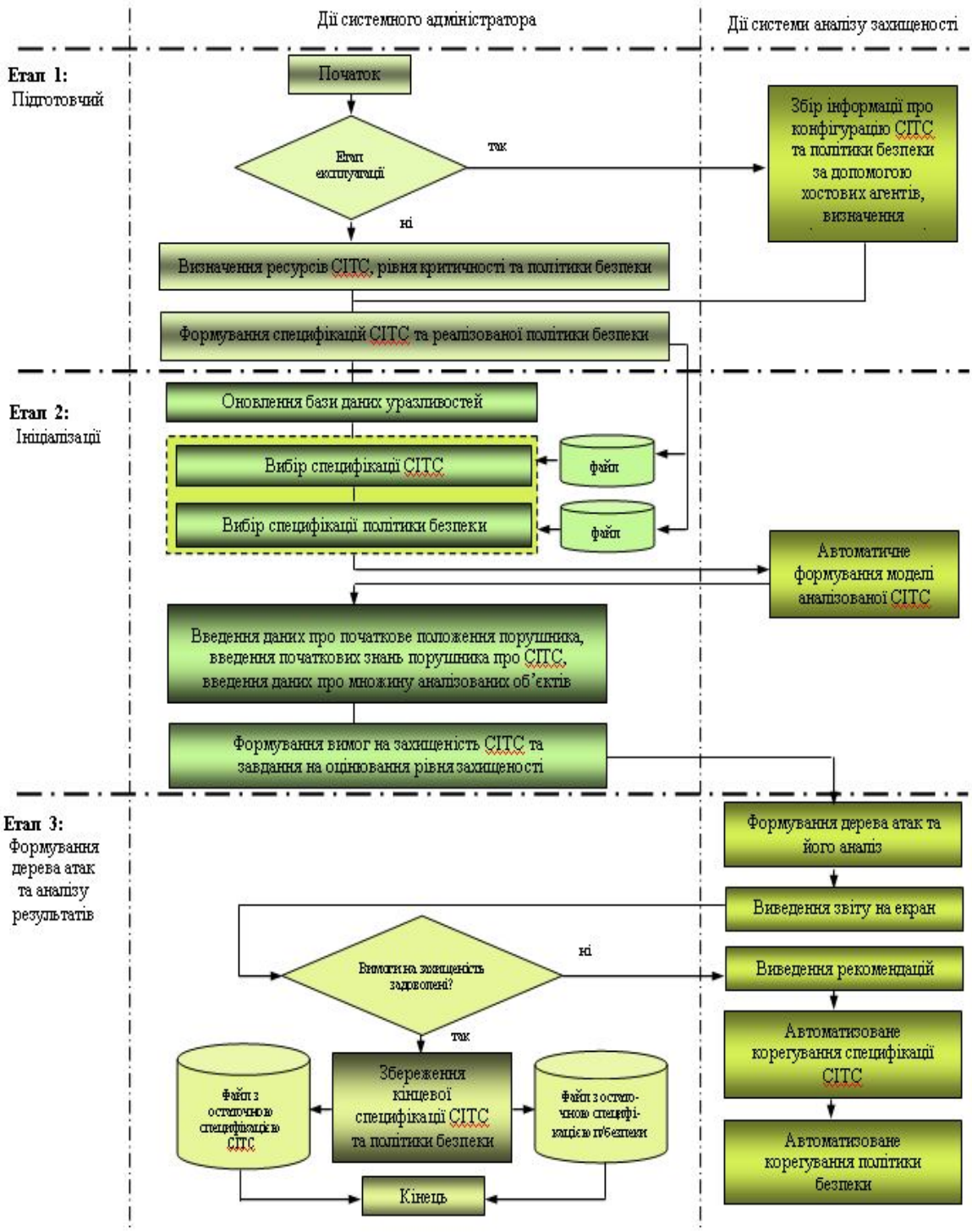

Рис. 1. Алгоритм аналізу захищеності СІТС

Наряду із загрозами безпеці інформації в СІТС, що були розглянуті вище та які полягають у порушенні конфіденційності, цілісності і доступності інформаційних об'єктів у окремий клас загроз варто виділити події, які залежно від умов можуть вплинути на кожну з відомих складових безпеки інформації шляхом:

— внесення деструктивних дій у технологію обробки даних;

— несанкціонованого доступу до ресурсів обчислювальної мережі без використання штатних засобів обчислювальної техніки;

— несанкціонованого включення до складу комплексів засобів обробки й захисту інформації нових елементів або зміни режимів їхньої роботи;

— виконання програм або дій в обхід системи захисту;

— підбору, перехоплення, розголошення або використання нестійких параметрів автентифікації і ключів шифрування (дешифрування);

— нав'язування раніше переданого або помилкового повідомлення, заперечення факту його передачі або прийому;

— некомпетентного використання, настроювання або адміністрування комплексів засобів обробки і захисту інформації тощо.

За принципами, характером та способами активного впливу на певний об'єкт, який може перебувати у стані зберігання, обробки або передачі інформації між вузлами СІТС або усередині вузла, такі події можуть бути поділені на загрози, що: 1) використовують принцип доступу суб'єкта СІТС (користувача, процесу) до певного об'єкта (файлу даних, каналу зв'язку) або до прихованих каналів, тобто шляхів передачі інформації; 2) забезпечують активний або пасивний впливи на складові безпеки інформації в СІТС; 3) реалізують опосередкований та безпосередній впливи, а також вплив на систему дозволів в СІТС.

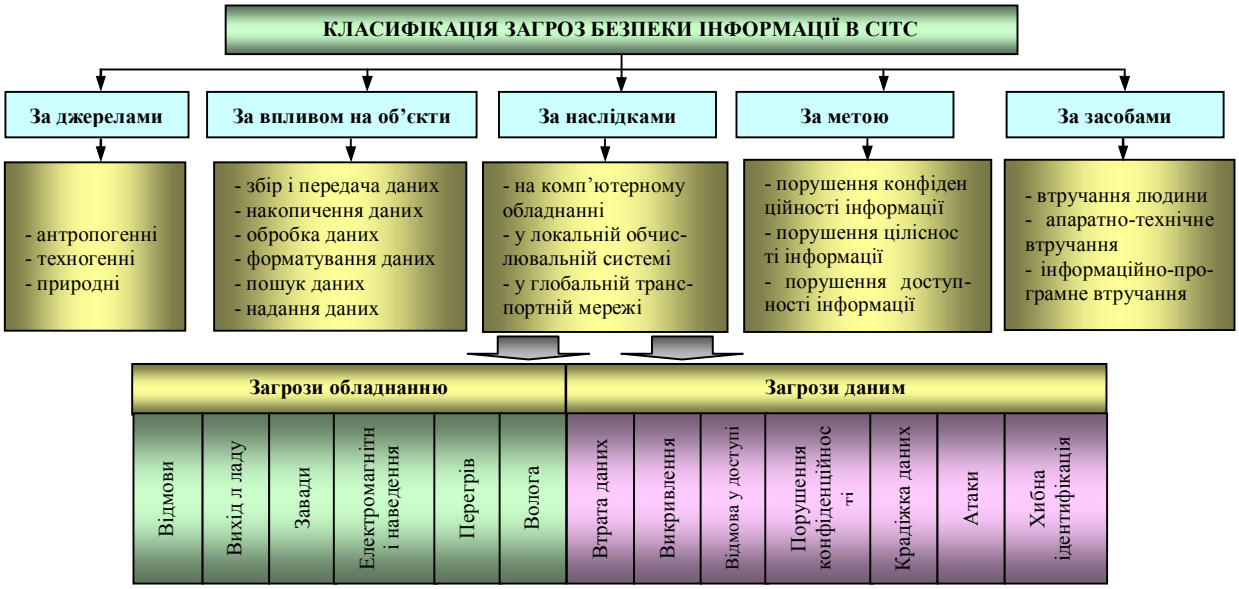

Рис. 2. Загальна класифікація комп'ютерно-телекомунікаційних загроз

До перерахованих вище загроз інформаційної безпеки варто додати ще й такі, як: загроза несанкціонованого обміну інформацією між користувачами; загроза відмови від інформації, тобто невизнання одержувачем (відправником) факту її одержання (відправлення); загроза відмови в обслуговуванні тощо.

Всі вони можуть бути віднесені до розряду як навмисних (табл. 1), так і випадкових загроз (табл. 2). На початку 2011 року компанія ESET [11] опублікувала список найпоширеніших Internet-загроз, виявлених фахівцями її вірусної лабораторії за допомогою технології раннього виявлення ThreatSense.Net.

Згідно нього лідером у російській двадцятці шкідливого ПЗ у першій декаді нового року стало сімейство Win32/Spy.Ursnif.A з показником поширеності у 3,62%, що на 0,07% більше, ніж в останню декаду 2010 року. Цей клас зловмисного ПЗ краде персональну інформацію й облікові записи із зараженого комп'ютера, після чого відправляє їх на вилучений сервер. Друге місце рейтингу належить загрозі INF/Autorun, частка проникнення якої знизилася на 0,87% і склала 3,54%. Цей тип шкідливих програм використовує для проникнення на комп'ютер користувача функцію автозапуску *Windows Autorun* і поширюється через змінні носії. На третє місце вийшли програми, що провокують користувачів відправити *SMS*-повідомлення на певний номер для одержання нібито

бажаного контента. Почесне місце у російській двадцятці займає шахрайська програма *Win32/Packed.ZipMonster.A*, що маскується під піратський контент у вигляді архіву. Окрім неї відзначається підвищена активність й інших програм, що увійшли в російський рейтинг найпоширеніших загроз: *Win32/RegistryBooster* (0,86%), *Win32/Hoax.ArchSMS.EP* (0,77%), *Win32/HackKMS.A* (0,76%), *Win32/Hoax.ArchSMS.ER* (0,73%). Рівень зростання присутності кожної із цих загроз склав близько 0,1%. Десяте місце займає загроза *PDF/Exploit.Pidief.PDS.Gen* з показником в 1,00%. У той же час, залишаються популярними шкідливі експлойти для платформи *Java*. Так, наприклад, шкідливе ПЗ *Java/Exploit.CVE-2010-0094.C*, що експлуатує уразливість *CVE-2010-0094*, дотепер є присутнім у рейтингу із часткою поширення в 0,6%.

Типи навмисних загроз безпеки інформації в СІТС Таблиця 1

Тип навмисної загрози	**Причини або спонукальні мотиви**
Розкрадання носіїв інформації	Прагнення використовувати конфіденційну інформацію у своїх цілях
Застосування програмних пасток	
Використання програм типу “троянський кінь”	Завдання збитків шляхом несанкціонованого доступу в систему
Помилки в програмах обробки інформації	Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп’ютерного вірусу	Руйнування інформаційної системи з метою завдання збитків
Помилкова комутація в мережі ЕОМ	З метою створення каналу для витоку конфіденційної інформації
Примусове електромагнітне опромінення	Вивід з ладу інформаційної системи з метою завдання збитків
Використання акустичних випромінювань	Одержання конфіденційної інформації
Копіювання за допомогою візуального й слухового контролю	
Маскування під користувача, підбор пароля	Несанкціоноване втручання в роботу системи в злочинних цілях
Помилки програміста: опис і перекручування програмного захисту, розкриття кодів та паролів	З метою добування особистої вигоди або завдання збитків
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація	

Що стосується десяти найпоширеніших загроз у світі, то в рейтингу першої декади 2011 року згідно даних [11] перше місце знову ж таки належить хробаку *Win32/Conficker* з відсотком проникнення в 5,38%, що ненабагато випереджає попереднього лідера – сімейство шкідливих програм *INF/Autorun* (5,30%).

Таблиця 2

Типи випадкових загроз безпеки інформації в СІТС

Тип випадкової загрози	**Причини або спонукальні мотиви**
Несправність апаратури, що може ініціювати несанкціоноване зчитування інформації	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Помилки в програмах обробки інформації	Застосування несертифікованого програмного продукту
Впровадження комп’ютерного вірусу	Не дотримання обслуговуючим персоналом вимог безпеки, порушення ним технологічної послідовності роботи із системою
Помилкова комутація в мережі ЕОМ	Низька кваліфікація обслуговуючого персоналу
Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування інформаційної системи або її створення
Перехресні наведення за рахунок ЕМВ	
Помилка в роботі оператора	Низька кваліфікація оператора, застосування несертифікованого програмного продукту

Тип випадкової загрози	Причини або спонукальні мотиви
Помилки технічного персоналу: перекручування схем захисту, помилкова комутація	Недостатня кваліфікація, порушення технології
Помилки користувача	Використання недостатнього захисту

Третє місце світової десятки займає загроза *Win32/PSW.OnLineGames*, що використовується хакерами для крадіжки аккаунтів гравців багатокористувальницьких ігор, з показником поширеності в 2,17%. У цілому ж світовий рейтинг найпоширеніших *Internet*-загроз нині включає: *Win32/Conficker* – 5,38%; *INF/Autorun* – 5,30%; *Win32/PSW.OnLineGames* – 2,17%; *Win32/Sality* – 1,82%; *INF/Conficker* – 1,39%; *Win32/Bflient.K* – 1,19%; *Win32/Tifaut.C* – 1,09%; *HTML/ScrIngect.B* – 0,84%; *Win32/Spy.Ursnif.A* – 0,83%; *Java/TrojanDownloader.Agent.NCA* – 0,76%.

Нейтралізація цих та інших, ним подібних загроз безпеки інформації у СІТС має здійснюватися виключно **службами безпеки** цих систем й забезпечуватись **механізмами реалізації функцій цих служб**, що мають бути представлені відповідними, переважно програмно-технічними засобами – механізмами шифрування, цифрового підпису, контролю доступу, забезпечення цілісності даних, забезпечення автентифікації, підстановки трафіку, керування маршрутизацією, арбітражу тощо. Якщо вести мову конкретно про загрози безпеці інформації в СІТС за метою реалізації, то з метою забезпечення конфіденційності й цілісності інформації у системі за рахунок унеможливлення доступу до неї та модифікації неавторизованим користувачем її змісту, окрім заходів організаційного обмеження доступом, необхідно перш за все застосовувати засоби: адміністрування доступу, управління фізичним доступом, криптографічного перетворення, контролю цілісності та охоронної сигналізації.

З метою недопущення переводу ресурсу в режим штучної відмови – порушення доступності об'єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, необхідно додатково передбачити механізми: запобігання постійного чи занадто тривалого використання такого ресурсу, забезпечення стійкості та відновлення процесів в умовах збоїв, резервування інформаційних об'єктів, аналізу потоків запитів від суб'єктів ЛОМ та телекомунікаційних мереж, контролю та поновленню цілісності інформаційних об'єктів (наприклад, в каналах СІТС).

Висновок. Зважаючи на те, що в сучасних умовах саме інформація стала найважливішим стратегічним ресурсом, а найбільший воєнно-політичний, економічний та соціальний успіх спостерігається перш за все там, де активно використовуються новітні інформаційні та телекомунікаційні засоби і послуги, – створення якісного та ефективного інформаційно-телекомунікаційного середовища для нашої держави є нині завданням найактуальнішим. Його позитивне вирішення створить передумови для активізації та стимулювання науки, економіки, бізнесу і медицини, дасть можливість істотно вплинути на посилення обороноздатності України та забезпечити:

— комплексну обробку відомостей про потенціального противника (конкурента), свої можливості та оточуюче середовище в інтересах підтримки прийняття раціональних управлінських рішень в реальних умовах обстановки та у реальному масштабі часу;

— стійкість та ефективність системи оперативного управління за рахунок підвищення ступеня живучості, надійності, завадо-захищеності та інформаційної безпеки використовуваних у ній технічних засобів;

— взаємодію та спільне використання різнорідних сил і засобів у рамках єдиної системи оперативного управління за рахунок зменшення участі людини в зборі, обробці, аналізі та розподіленні інформації тощо.

Разом з тим стрімкий розвиток комп'ютерних технологій дасть можливість протиборчим сторонам збільшити швидкість доступу до відкритих і відносно-відкритих джерел інформації один одного, а також проводити додаткові заходи з добування, вивчення та обробки відомостей стосовно існуючого і вірогідного противника (конкурента), використовуючи для цього такі методи, як розвідка в системах телекомунікацій, мережна розвідка та комп'ютерна або інакше кіберрозвідка. При цьому основними джерелами

проникнення до СІТС, як правило, виступатимуть [4-6]: хакери (зломщики СІТС); звільнені або скривджені співробітники; професіонали-фахівці, що присвятили себе шпигунству; конкуренти, ступінь небезпеки яких залежить від цінності інформації, до якої вони мають доступ та від рівня їхнього професіоналізму тощо. За даними американського Інституту комп'ютерної безпеки, ними останнім часом найбільш широко використовуються такі методи, як: підбір ключів (паролів) - 13,9% від загальної кількості; заміна *IP*-адреса - 12,4%; ініціювання відмови в обслуговуванні - 16,3%; аналіз трафіку - 11,2%; сканування - 15,9%; підміна даних, що передаються мережею - 15,6%; інші методи - 14,7%.

Такий стан справ свідчить про складність визначення можливих загроз безпеки інформації в СІТС і способах їхньої реалізації та дає можливість зробити висновок про те, що універсального способу захисту, який запобіг би будь-якій загрозі нині, нажаль, не існує. Нейтралізація загроз безпеки має здійснюватися виключно службами безпеки СІТС й забезпечуватись механізмами реалізації функцій цих служб.

ЛІТЕРАТУРА

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", № 80/94-ВР від 5.07.1994
2. Закон України "Про телекомунікації", № 1280-IV від 18.11.2003.
3. Биячуев Т.А. Безопасность корпоративных сетей. / под ред. Л.Г.Осовецкого. – СПб: СПб ГУ ИТМО, 2004. – 161 с.
4. Безбогов А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А.Безбогов, А.В.Яковлев, В.Н.Шамкин. – Тамбов: Изд-во Тамб.гос.тех.ун-та, 2006. – 196 с.
5. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навчальний посібник. – Харків: Консул, 2005. – 576 с.
6. Сычев Ю.Н. Основы информационной безопасности. Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. – 300 с.
7. Степашкин М.В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак /И.В.Котенко, М.В. Степашкин // Труды международной научной школы "Моделирование и анализ безопасности и риска в сложных системах". – Спб., 2006. – С.150 – 154
8. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: Изд-во ДиаСОФТ, 1999. – 992 с.
9. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. Под ред.В.А.Хорошко. – К.:Арий, 2008. – Том 1, - 464 с. – Том 2, 344 с.
10. Василенко В.С., Бордюк О.С., Полонський С.М. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/ 64068.doc.htm
11. Eset: мировая двадцатка интернет-угроз в январе. [Електронний ресурс]. – Режим доступу: http://it-sektor.ru/Mirovaya-dvadtscatka-internet-ugroz-v-yanvare.html

Надійшла: 20.09.2011

Рецензент: д.т.н., проф. Конахович Г.Ф.