ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА: АНАЛІЗ І КЛАСИФІКАЦІЯ ВПЛИВІВ НА АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Іванюта Т.М. Національний університет харчових технологій
Мочалюк В.В. Національна академія оборони України

Дана робота присвячена аналізу можливостей здійснення різноманітних впливів на автоматизовані інформаційні системи (АІС) підприємств і запропоновано їх класифікацію. Визначені класифікаційні ознаки в подальшому можуть бути використані для визначення системи показників оцінки інформаційної захищеності підприємств та визначення критеріїв оптимальності захищеності підприємства.

Ключові слова: інформація, автоматизовані інформаційні системи підприємства, вплив, інформаційна безпека.

The given work is devoted to the analysis of possibilities of realization of various influences on the automated informative systems (AIS) of enterprises and their classification is offered. Definite classification signs in future can be used for determination of the system of indexes of estimation of informative protected of enterprises and determination of criteria of optimum of protected of enterprise.

Keywords: information, automated informative systems of enterprise, influencing, informative safety.

Вступ. На сучасному етапі розвитку суспільства інформація стає головним ресурсом науково-технічного і соціально-економічного прогресу світової спільноти, створює інтелектуальний фундамент для вирішення багатьох глобальних проблем сучасності [1].

Перехід інформації в розряд найважливіших ресурсів людства викликає до життя проблему боротьби за володіння цим ресурсом, і, як наслідок, появу принципово нових засобів нападу і захисту – інформаційної зброї.

В рамках інформаційної боротьби між підприємствами, як і при інших конфліктних діях, можна виділити оборонну і наступальну складові.

Оборонна складова реалізується методами забезпечення безпеки і інформаційної протидії, а наступальна, пов'язана з розробкою і використовуванням інформаційної зброї, може розглядатися як вплив на автоматизовані інформаційні системи (АІС) через мережні з'єднання, активний пошук і виявлення несанкціонованих дій в автоматизованих інформаційних системах[2].

Ведення інформаційної війни між підприємствами має на увазі злагоджену діяльність по використовуванню інформації як зброї. Це суперництво і організовані дії конфліктуючих сторін в галузі інформаційних потенціалів, що проводяться з метою зниження можливостей по використовуванню наявних економічних і наукових потенціалів конкурента і збереження, чи навіть підвищення можливостей по використовуванню своїх потенціалів.

Об'єктом уваги при веденні інформаційної війни стають автоматизовані інформаційні системи і мережі обміну інформацією (включаючи відповідні лінії передач, оброблювальні центри і людські чинники цих систем), а також інформаційні технології, що використовуються на підприємствах[3].

Постановка проблеми. Аналіз літератури з безпеки інформації і хакінгу не виявив будь-якої всеохоплюючої класифікації впливів на АІС. Це зумовлено тим, що під час аналізу інформаційної безпеки підприємств розглядаються лише механізми проведення впливів на АІС і їх наслідки, як і в літературі присвяченій безпосередньо хакінгу. Тому аналіз і класифікація впливів на комп'ютерно-інформаційну безпеку підприємств є актуальним завданням.

Результати дослідження. Перш за все необхідно розділити впливи на АІС які здійснюються за безпосереднім фізичним доступом до ресурсів АІС і впливи, які засновані на логічному подоланні системи захисту АІС за

допомогою програмно-математичних засобів, тобто за принципом здійснення впливу.

1. За принципом здійснення впливу:

1.1. фізичний: 1.1.1. подолання межі територіального захисту і доступ до незахищених інформаційних ресурсів; 1.1.2. викрадення документів і носіїв інформації; 1.1.3. візуальне перехоплення інформації, що виводиться на екрани моніторів і принтери а також прослуховування; 1.1.4. перехоплення електромагнітних випромінювань;

1.2. логічний: 1.2.1. за розміщенням АІС підприємства відносно джерела впливу; 1.2.2. за характером взаємодії з АІС підприємства; 1.2.3. за об'єктом впливу; 1.2.4. за безпосереднім об'єктом впливу; 1.2.5. за рівнем автоматизації; 1.2.6. за типом використання недоліків системи захисту АІС підприємства; 1.2.7. за рівнем еталонної моделі.

Фізичний вплив, це вплив, який здійснюється безпосередньо на об'єкти АІС підприємства. Він можливий, тільки в разі наявності фізичного доступу до ресурсів та об'єктів АІС підприємства.

Під інформаційним нападом розуміється здійснення впливу на АІС підприємства.

Вплив у відповідь на інформаційний напад здійснюється після виявлення факту інформаційного нападу на об'єкт АІС і ідентифікації противника. В разі правильно спланованого впливу ефективність здійснення впливу у відповідь дуже незначна[4].

2. За характером дії: 2.1.пасивний; 2.2.умовно пасивний; 2.3. активний.

Пасивна дія не чинить безпосереднього впливу на роботу АІС підприємства, але може порушити її політику безпеки.

Активні дії мають на меті нанесення прямої шкоди АІС підприємства, та полягають у порушенні конфіденційності, цілісності і доступності інформації, а також виводять з ладу комп'ютерні телекомунікації і здійснюють психологічний вплив на користувачів АІС підприємства.

Умовно пасивні дії, мають на меті підготовку до активної дії. Вони спрямовані на ведення комп'ютерної розвідки і подолання системи захисту АІС підприємства.

3. За типом загрози інформації, яку реалізує вплив: 3.1.порушення конфіденційності (розкриття); 3.2.порушення цілісності; 3.3.порушення доступності.

Ця класифікаційна ознака є прямою проекцією трьох основних типів загроз інформації – розкриття, порушення цілісності і порушення доступності.

4. За метою впливу: 4.1.прослуховування; 4.2.неавторизований доступ; 4.3.виведення з ладу.

Як і попередня, ця класифікаційна ознака є прямою проекцією трьох основних типів загроз. Але вона відображає цілі, які переслідуються при здійснені впливу, тоді, як попередня відображає наслідки, до яких може призвести той, чи інший вплив.

Так при прослуховуванні виникає порушення конфіденційності чи ресурсів АІС підприємства. При неавторизованому доступі можливо реалізувати будь який з типів загроз. Виведення з ладу реалізує тип загрози – порушення нормальної роботи АІС підприємства.

5. За сценарієм: 5.1.без попереднього збору інформації про АІС підприємства; 5.2.з попереднім збором інформації про АІС підприємства; 5.3.зі збором інформації про АІС підприємства під час впливу.

В загальному випадку для здійснення вдалого впливу необхідно знати структуру захисту АІС на яку здійснюється вплив, тому перед атакою необхідно проводити додаткові заходи для визначення структури захисту. Іноді в зв'язку з браком часу збір інформації про АІС підприємства відбувається під час впливу, але існують атаки, які здійснюються без збору інформації про АІС. В більшості випадків такі впливи носять випадковий характер і пов'язані з неконтрольованим розповсюдженням засобів впливу у вигляді вірусів.

6. За рівнем здійснення впливу: 6.1.фізичний; 6.2.синтаксичний; 6.3.семантичний.

Впливи на фізичному рівні, це впливи, які призводять до порушення чи припинення роботи техніки і телекомунікаційних мереж.

Синтаксичні впливи спрямовані на порушення роботи математичного (програмного) забезпечення.

Впливи на семантичному рівні не порушують порядок роботи програмного забезпечення, але призводять до того, що результати роботи (відповіді, рекомендації, прогнози та інше) програмних засобів не відповідають дійсності. Найчастіше до такого впливу схильні експертні системи, системи підтримки прийняття рішень, автоматизовані системи ситуаційного аналізу, системи імітаційного моделювання[5].

Загальна схема запропонованої класифікації впливів на АІС підприємств наведена на рис 1.

Наступним кроком необхідно розглянути логічні впливи, як найпотужніше джерело витоку інформації.

Логічні впливи можливо класифікувати за наступними признаками:

1. За розміщенням АІС підприємства відносно джерела впливу: 1.1.джерело впливу знаходиться в межах одного сегменту АІС підприємства; 1.2.джерело впливу і АІС підприємства знаходяться в різних сегментах.

Якщо в першому випадку вплив здійснюється безпосередньо з будь якої точки локальної мережі підприємства, то в другому випадку вплив здійснюється з відкритої мережі на закриті мережі, які мають обмежений доступ.

Вплив, який здійснюється в межах одного сегмента не потребує подолання міжсегментного захисту АІС підприємства, тому вплив такого типу здійснити значно легше ніж зовнішній. Але при цьому зовнішній віддалений вплив несе значно більшу загрозу. Це пов’язано з тим, що у випадку атаки між сегментами, АІС підприємства і атакуючий можуть знаходитись на віддалені тисяч кілометрів, що значно ускладнює можливість виявлення атакуючого, а відповідно і заходи попередження і відповіді на такі впливи.

2. За характером взаємодії з АІС підприємства: 2.1.інтерактивний вплив; 2.2.безумовний вплив.

У першому випадку атакуючий виконує постійне спостереження за станом АІС підприємства, і при виникнення певної події, наприклад запит певного типу, розпочинається вплив.

У випадку безумовного впливу початок впливу безумовний по відношенню до цілі, тобто вплив виконується негайно і безвідносно до стану АІС підприємства.

3. За об'єктом: 3.1.спрямований на певний об'єкт; 3.2.без спрямованості на об'єкт.

Як правило атакуючий повинен мати інформацію, про об'єкт впливу і про систему його захисту. Але в певних випадках існують впливи без спрямованості на певний об'єкт. Такі пливи виникають в разі некерованого розповсюдження засобів впливу у вигляді вірусів.

4. За безпосередніми об'єктами впливу: 4.1.вплив на постійні компоненти системи захисту; 4.2.вплив на змінні елементи системи безпеки; 4.3.вплив на протоколи взаємодії; 4.4.вплив на функціональні елементи комп'ютерної системи.

Кінцевим об'єктом впливу завжди є інформація, що захищається. Під безпосереднім об'єктом впливу розуміється об'єкт, аналіз якого, використовується при реалізації засобів здійснення впливу на АІС підприємства.

5. За типом використання недоліків системи інформаційно-комп'ютерної безпеки підприємства: 5.1.впливи засновані на помилках адміністративного управління; 5.2.впливи засновані на недоліках алгоритмів захисту, які реалізовані в засобах захисту АІС підприємства.

Під помилками адміністративного управління розуміють некоректно обрану політику безпеки АІС підприємства чи помилки в проекті реалізації обраної політики безпеки. Ефективні засоби впливу можуть бути також засновані на недоліках алгоритмів захисту і помилках реалізації певних пристроїв захисту.

6. За рівнем автоматизації: 6.1.з постійною участю людини; 6.2.за допомогою спеціально розроблених програм, з участю людини в якості особи,

що приймає рішення в разі виникнення суперечливої ситуації; 6.3.за допомогою спеціально розроблених програм, без участі людини.

В першому випадку вплив базується на знаннях людини, яка його здійснює, і має дуже високий рівень знань з питань комп'ютерної інженерії. В другому випадку людина виступає в якості експерта, і визначає загальні напрямки здійснення впливу, що не потребує дуже високих знань в області комп'ютерної інженерії, а потребує лише розуміння загальних принципів. В третьому випадку впливу повністю здійснюється програмними засобами, тому його розвиток і наслідки є некерованими, і повністю залежать від розробника відповідної програми.

7. За рівнем еталонної моделі: 7.1.фізичний; 7.2.канальний; 7.3.мережний; 7.4.транспортний; 7.5.рівень сеансів; 7.6.прикладний; 7.7.рівень представлень.

Будь який протокол обміну, як і будь яку мережну програму, можна спроектувати на семирівневу еталонну модель ISO/OSI [6, с.82-91]. Така багаторівнева проекція дозволяє описати в термінах еталонної моделі ISO/OSI функції, які закладені в мережний протокол чи програму. Вплив також є програмою з використанням мережних технологій. У зв'язку з цим є логічним розглядати вплив на АІС підприємства у відповідності до еталонну моделі ISO/OSI.

Загальна схема запропонованої класифікації логічної складової впливу на АІС підприємств наведена на рис 2.

Висновок. Таким чином в наведеній роботі було проаналізовані різноманітні можливості здійснення впливу на АІС підприємств і запропоновано класифікацію впливів на АІС підприємств. Окремо розглянуто логічну складову впливу, як найпотужнішого джерела витоку інформації і запропоновано класифікацію логічної складової впливу на АІС підприємства.

Визначені класифікаційні ознаки в подальшому можуть бути використані за напрямками:

1. детального аналізу відомих впливів;

2. прогнозування подальшого розвитку інформаційного протиборства між підприємствами;
3. визначення системи показників оцінки інформаційної захищеності підприємств;
4. Визначення критеріїв оптимальності захищеності підприємства.

Список використаних літературних джерел

1. Волковский Н.Л. История информационных воен. В 2 ч. Ч.2 / СПб.: ООО «Издательство Полигон», 2003.

2. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд „Университет”, 2000.

3. Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. – М.: Финансы и статистика, 1989. – 351 с.

4. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива // http://www.agentura.ru/equipment/psih/info/war/.

5. Гриняев С.Н. Особенности информационной войны во время агрессии НАТО против Югославии (по материалам открытой печати) // http:// www.agentura.ru/equipment/psih/info/yugoslav/.

6. Э. Таненбаум, М. ван Стеен Распределенные системы. Принципы и парадигмы. – СПб.:Питер, 2003. – 877с.

Рис. 1 Класифікація впливів на АІС підприємств.

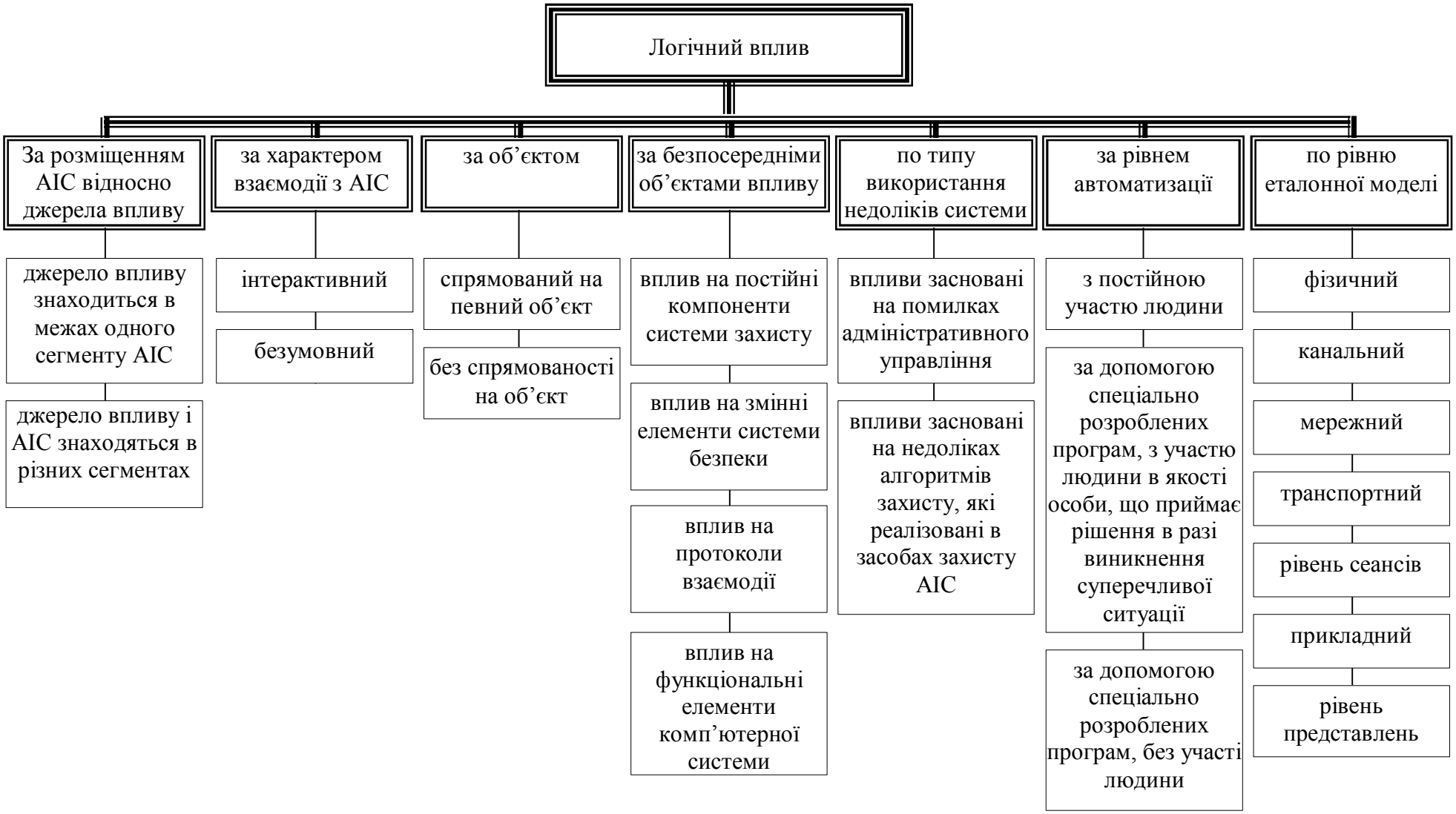

Рис. 2 Класифікація логічної складової впливу на АІС