ВПЛИВ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА НА ПРИНЦИПИ ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ

Романюков М.Г.
науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук

Вступ. «Однією з основних реальних потенційних загроз національній безпеці України у інформаційній сфері, є розголошення інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів держави та суспільства» [1].

На сьогодні можна спостерігати наступний перехідний період функціонування людства в соціумі до інформаційного суспільства та суспільства високих технологій. Інформаційні технології, виходячи на промисловий рівень, наділяють інформацію новими функціями засобів виробництва, сировинної бази, видами продуктів та товарів повсякденного вжитку. Дані зміни несуть за собою втручання в усі сфери державної життєдіяльності (економічні, політичні та ін.) навіть змінюючи соціум, як інститут. Змінюється образ кожного індивида, його особистості та світогляду. Разом з глобальним оцифровуванням змінюється звична парадигма соціальної реальності пов'язаної з доставкою, обробкою, реагуванням та контролем інфорсвційних потоків [1].

Виникає нова інформаційна зброя, така як вміння маніпулювати інформацією та дезінформацією. Як пише The Times:"Планету чекає зміна парадигми, на стільки ж радикальна, як зміна

кавалерії на танки. Застосування дезінформації для зриву демократичних дебатів, кібератаки, економічна політика з метою тиску, розгортання не декларованих військ, які стають поштовхом до більш стандартного військового втручання. Ситуація, коли на війні зброєю стає що завгодно [2].”

Виникають наступні проблеми, що стосуються насмперед забезпечення безпечного впливу глобальних змін на трансформацію сфери інформаційної безпеки та засекречування інформації. Нову еру вразливостей починають формувати нематеріальні цінності та модифікована структура активів, що вимагає нових ідей при вирішенні питань технології захисту [4].

Історичні етапи технології засекречування. Відповідно до А. Денисова основною технологією влади, що вимагає захисту, належить управління поведінкою вибору. Даний вибір є притаманним людству, суть якого і є влада. На цілі засекречування мали вплив різні історичні епохи. У зв’язку з цим є доцільним розглянути чотири історичні періоди, у яких новий етап технологічної революції супроводжувався приходом до влади нового правлячого класу [3]:

- епоха 1, феодальне або кріпосне (до індустріальне) суспільство;
- епоха 2, індустріальне буржуазне (або соціалістичне) суспільство;
- епоха 3, постіндустріальне, перехідне до інформаційного суспільства, (інвестиційна фаза);
- епоха 4, суспільство високих технологій, винайдених у інноваційній фазі.
- Оскільки від трансформації технологій поведінки вибору залежать об’єкти, цілі та принципи засекречування, виникає необхідність їх розглянути:
- епоха 1, робота в умовах ручної праці, що є примусовою. За А. Денисовим вона характеризується як управління міжособистісних комунікацій думок і роботи.
- епоха 2, має прерогативу «стимул- реакція», в умовах вільного продажу праці на ринку праці. Важка фізична

праця починає механізуватися, а на пізніших етапах автоматизуватися. Розглядаючи дану епоху в рамках сучасних теорій, можна зробити висновок що на сьогодні вона знаходить відображення у кібернетиці 1-го порядку.

- епоха 3 являє собою рефлексію управління на рефлексії свідомості, що супроводжується дотриманням прав людини, роботизацією важкої, небезпечної для здоровя праці. На поглибленому етапі починає автоматизуватися розумова праця. Відбувається зародження технократичного способу мислення [4]. За А. Денисовим, дане управління має на меті використання концепції єдиної індивідуальної свідомості. В сучасних теоріях дана епоха знайшла відображення у рефлексивному управлінні за принципом кібернетики 2-го порядку та вищих аналогів з описом систем із самосвідомістю.
- епоха 4 рефлексивне управління поведінкою вибору за моделлю рефлексії свідомості з використовуванням, по А. Денисову, концепції множинності шарів індивідуальної свідомості. Епоха характеризується як назріваюча інтелектуально-гуманітарна революція.

Оскільки зі зміною залежності об'єктів, цілей та принципів засекречування від технологій поведінки відбувається трансформація предмету та засобів управління вибором, то виникають наступні предмети і засоби управління за епохами:

1. Управління змістом між особистого інформаційного обміну за допомогою сили;
2. Управління каналами, характером і трафіком між особистого інформаційного обміну за допомогою законодавчих, організаційних, технічних а також соціально-психологічних засобів;
3. Рефлексивне управління усвідомленням поведінки вибору, заснованому на математичних моделях морального вибору, за допомогою маніпулювання здатністю до міжособистного інформаційного обміну;
4. Рефлексивне управління усвідомлення вибору за допомогою маніпулювання здатністю до між особистого (не

відомого спостерігачеві) інформаційного обміну за допомогою технологій психоінжинирінгу [3].

Ієрархічна модель системи засекречування. Системи захисту інформації, а далі системи інформаційної безпеки розвивались так, що базові принципи, методи і засоби, напрацьовані на попередніх етапах, не відкидаються, а залишаються, розширюються або удосконалюються, знаходячи собі свою нішу у нових комплексних системах інформаційної безпеки. Більше того набувають подальшого розвитку та вдосконалення, що можна спостерігати при побудові комплексних систем захисту інформації. При цьому має місце принцип повноти та неперервності захисту, як окремої комплексної системи захисту, так і засекречування вцілому. Розглядаючи ієрархічну систему засекречування, можна спостерігати наступну можливість – секрет верхнього рівня може розділятись на нижньому рівні. Цим можна понизити рівень захищеності кожного з розподілених секретів, полегшивши задачу оптимізації всієї системи засекречування.

Цілі засекречування за А. Денисовим розподіляється за рівнем системи засекречування:

1. Засекречування інформаційних потоків
2. Засекречування трафіку та каналів обміну інформаційними пакетами, засекречування моделей та технологій обміну;
3. Засекречування матриць цінностей;
4. Засекречування картин бачення світу.

Систему засекречування можна відобразити у чотирьох рівневій ієрархічній структурі (рис. 1). Розгладаючи дану модель можна сформувати систему чотиритсупеневої системи захисту державної таємниці. На першому рівні необхідно захищати відомості, що закріплені в ЗВДТ. На другому рівні відбувається захист трафіку, моделей та обміну пакетими. Третій рівнень відповідає за захист матриць цінностей. Метод даного захисту полягає у маніпулюванні здатністю до між особистого інформаційного обміну. Четвертий рівень потребує глибоких

досліджень, та буде побудований на принципі систем інтерпретації даних (зокрема віртуальних), що сприймаються органами почуттів людини.

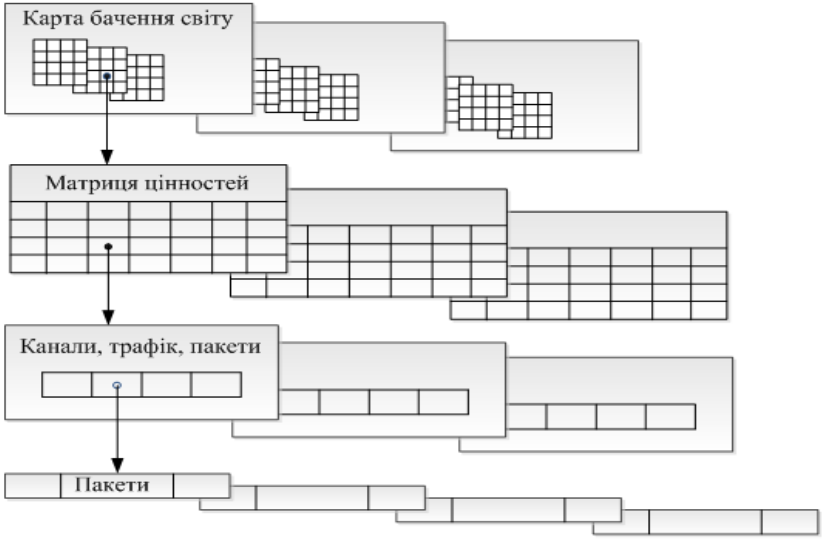

Рис. 1. Характеристика ієрархічної чотириступеневої моделі засекречування.

Висновки. Проаналізувавши модель розвитку суспільства, запропоновано принципи моделі ієрархічної системи засекречування. Дана модель має чотири рівні: на першому рівні засекречуються інформаційні потоки, на другому – моделі та технології обміну інформаційними пакетами, на третьому – має місце засекречування матриць цінностей, на четвертому – відбувається засекречування картин бачення світу. Запропонована модель розкриває можливості до створення більш детальних та обґрунтованих засобів засекречування. Отримані результати дають можливість вдосконалити засоби національної та інформаційної безпеки та відкривають нові напрямки досліджень по створенню ефективних систем захисту правоохоронної діяльності.

1. Корченко О.Г. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : Монографія / О.Г. Корченко, О.С. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.
2. Путин использует бойню в Украине, чтобы репетировать войну с Западом / The Times, 10 августа 2016. [Электронный ресурс] – Режим доступа: http://glavnoe.ua/news/n279723.
3. Денисов А.А. Нетократия и рефлексия: Засекречивание в постиндустриальном обществе / А.А Денисов // Рефлексивные процессы и управление. – Том 7, № 1, 2007. – С. 33-50.
4. Агеев А.И. Вектор перемен / А.И. Агеев, С.В. Авдеев, Рыжов В.Н. и др. // Экономические стратегии. – № 4, 2016. – С. 84-106.

ДО ПИТАННЯ ЗАХИСТУ СПЕЦІАЛІЗОВАНИХ КОРПОРАТИВНИХ МЕРЕЖ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Рудий А.Т.
військовослужбовець

Щур Є.Л.
інспектор відділу професійного навчання управління кадрового забезпечення ГУ НП у Волинській області

Бойчук Т.Я.
слідчий СВ Рожнятівського відділення поліції ГУ НП у Івано-Франківській області

Заєць Я.В.
здобувач освітнього ступеня магістр Львівського державного університету внутрішніх справ

Актуальність проблеми. З огляду на вимоги сучасного підходу до побудови надійної системи захисту інформаційних активів спеціалізованих корпоративних мереж (СКМ) Національної поліції України актуальним залишається розроблення ефективних механізмів захисту. Ефективність системи захисту СКМ залежить від прийняття виважених рішень які підтримують і