DOI:**10.33099/2311-7249/2023-46-1-51-55**

УДК: 004.056

Михайло Анатолійович Стрельбіцький *(доктор технічних наук, професор)*
Валентин Юрійович Мазур *(доктор військових наук, професор)*
Володимир Васильович Лемешко *(кандидат військових наук, доцент)*

Національна академія Державної прикордонної служби України імені Богдана Хмельницького

ПРОТОКОЛИ ОБМІНУ «АГРЕГОВАНОЇ» ІНФОРМАЦІЇ В ІНФОРМАЦІНО–ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

У статті, на підставі класифікації інформації з обмеженим доступом, визначені передумови порушення її конфіденційності у ході дотримання вимог політики безпеки інформаційно-телекомунікаційної системи. Визначено, що збільшення кількості інформації може призводити до підвищення рівня обмеження доступу. Для множин інформації такого типу дано визначення як «агрегованої». Наведені умови порушення безпеки інформації, рівень конфіденційності якої залежить від її кількості. Визначені можливі канали прихованого витоку інформації з вузлів мережі без порушення політики безпеки інформаційно-телекомунікаційної системи. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження нового протоколу обміну між вузлами інформаційно-телекомунікаційних систем. Розроблений протокол обміну «агрегованої» інформації між вузлами мережі передбачає використання контейнеру «агрегованої» інформації, який забезпечує формування інформації з вищим рівнем доступу на захищеному вузлі інформаційно-телекомунікаційної системи.

Ключові слова: *інформація, конфіденційність, протокол, інформаційна система.*

Вступ

Виконання Державною прикордонною службою України своїх основних функцій вимагає обробки значної кількості різнопланової інформації, в тому числі такої, що не має відповідно до законодавства грифу обмеження доступу. Разом із тим, зазначена інформація є власністю Державної прикордонної служби України (далі – Держприкордонслужба) і підлягає захисту. Безпека цієї інформації досягається дотриманням її властивостей, а саме: конфіденційності, цілісності, доступності та спостереженості [1]. Питання, що стосуються дотримання цілісності, доступності та спостереженості достатньо добре опрацьовані технологічно, зокрема, внаслідок резервування складових інформаційно-телекомунікаційних систем (далі – ІТС), розробки механізмів архівування та відновлення стану системи після збою тощо. Ключовим у підтриманні безпеки інформації залишається дотримання конфіденційності інформації.

Постановка проблеми. Керівними документами передбачена можливість формування кінцевого документу з вищим рівнем обмеження доступу із відомостей з нижчим рівнем. У процесі запровадження систем електронного документообігу для відомостей відкритого характеру можлива ситуація одночасного знаходження на одному вузлі мережі групи відомостей, що сукупно формують інформацію з вищим рівнем обмеження доступу. Вищенаведене вимагає пошуку процедурних і функціональних рішень унеможливлення знаходження на одному вузлі мережі такої групи інформації.

Аналіз останніх досліджень і публікацій. Аналіз публікацій у цій галузі [2–4] свідчить про існування багатьох методів, що регламентують доступ користувачів до ресурсів інформаційної системи. Зазначені методи формально обґрунтовані та унеможливлюють витік інформації за умов дотримання всіх вимог визначених обраним методом. У цьому контексті доцільно зауважити той факт, що доступ користувачів до ресурсів інформаційної системи є детермінований, тобто визначений до моменту ознайомлення користувача з інформацією, що є логічним. З вищенаведеного можна зробити логічний висновок, що з точки зору всіх систем розмежування доступу до ресурсів ІТС немає підстав обмежувати користувача в доступі до інформації якщо раніше такий доступ був наданий і жодних додаткових обмежень не було введено. У цьому контексті варто зауважити вимоги Зводу відомостей, що становлять державну таємницю [5], в якому за відповідними розділами регламентовано віднесення інформації до секретної та визначено її ступінь обмеження доступу. Аналіз цього документу показав, що агрегуючи інформацію з нижчим ступенем обмеження доступу, користувач ІТС може отримати інформацію з вищим ступенем обмеження доступу. Таким чином, збільшення кількості інформації в ІТС може призвести до формування даних з вищим ступенем секретності, при чому за повного дотримання вимог політики безпеки, яку визначає обрана система розмежування доступу.

Мета статті – визначення умов виникнення несанкціонованого каналу витоку службової інформації інформаційно-телекомунікаційних

системах Державної прикордонної служби України та формування безпечних протоколів обміну між вузлами ІТС.

Виклад основного матеріалу дослідження

Інформаційно-телекомунікаційні системи Держприкордонслужби використовують інтранет-мережу прикордонного відомства, що базується на орендованих каналах зв'язку національних операторів. Така структура відомчої телекомунікаційної мережі не передбачає доступу до інших інформаційних ресурсів поза межами інтранет-мережі. Разом із тим, у ході використання орендованих каналів при передачі даних немає гарантії факту не перехоплення пакетів та витоку будь-якої інформації, в тому числі такої, що не відноситься до інформації з обмеженим доступом.

В умовах обробки ІТС відкритої інформації (інформації, що не відноситься до інформації з обмеженим доступом), захист якої полягає тільки в забезпеченні дотримання її трьох властивостей (цілісності, доступності та спостережності), забезпечення конфіденційності не є обов'язковим (з причини загальнодоступності відкритої інформації). Постановою Кабінету Міністрів України зазначено, що «Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, що можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією» [6]. Зокрема, тим самим документом зазначено, що «захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації».

Саме тому, більшість ІТС Держприкордонслужби не має спеціалізованих технічних засобів захисту інформації та розгорнутої комплексної системи захисту інформації. Такий підхід є логічним з економічної точки зору – немає сенсу захищати інформацію, якщо доступ до неї відкритий. Враховуючи вищенаведене, отримання інформації з відкритих джерел або перехоплення трафіку в інтранет-мережі Держприкордонслужби є нескладним завданням.

Розглянемо узагальнену процедуру віднесення будь-якої інформації до інформації з обмеженим доступом. Відповідно до переліку відомостей, що становлять державну таємницю [5] державні експерти з питань таємниць визначають, яка саме інформація становить державну таємницю у визначених законодавством сферах. Аналогічний підхід застосовується щодо віднесення інформації до службової, зокрема, в Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України та Інструкції із захисту публічної інформації у Державній прикордонній службі України [7] зазначено, що право на прийняття рішення щодо розповсюдження службової інформації, власником якої є відповідні органи Держприкордонслужби, надати керівникам цих органів. Таким чином, відповідність інформації хоча б одному із пунктів наведених документів є підставою відповідній посадовій особі для надання документу, виробу чи іншого матеріального носія інформації, що містить ці відомості, грифа обмеження доступу.

Проведений аналіз розділів Зводу відомостей, що становлять державну таємницю та Переліку відомостей, що становлять службову інформацію у Держприкордонслужби показав наявність пунктів, що містять «агреговане» визначення ступеня обмеження доступу. Під «агрегованим» пунктом будемо розуміти таку величину кількості інформації попереднього рівня доступу, досягнення якої призводить до підвищення загального рівня обмеження доступу.

Аналіз розділів Зводу відомостей, що становлять державну таємницю показав наявність значної кількості «агрегованих» пунктів, тобто таких, у яких ступінь обмеження доступу підвищується залежно від кількості інформації (рисунок 1).

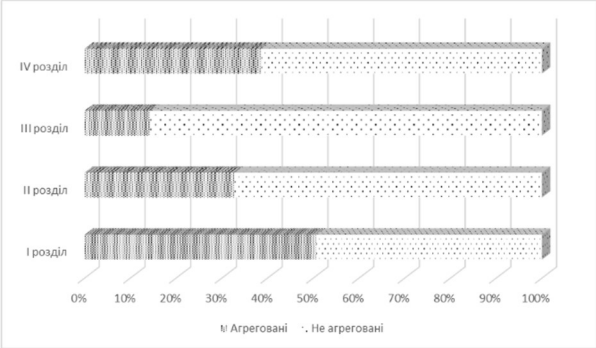

Рис. 1. Співвідношення агрегованих пунктів в ЗВДТ

Наведемо приклад «агрегації», пунктом 1.10.6 «Відомості про комплекс заходів інженерно-технічного облаштування державного кордону та прикордонної смуги…» частиною 3 «щодо ділянки відповідальності регіонального управління, органу охорони державного кордону, загону морської охорони, відділу прикордонної служби ДПС» передбачено присвоєння ступеня секретності «таємно». Разом із тим, пунктами 81 та 83 Наказу № 501 [7] передбачено віднесення інформації за окремими складовими, про заходи інженерно-технічного облаштування державного кордону на ділянці прикордонних підрозділів, до службової. Таким чином, сукупність службової інформації у кількості, що розкриває комплекс заходів інженерно-технічного облаштування державного кордону відділу прикордонної служби ДПС, повинна (відповідно вимог ЗВДТ) мати вищий рівень обмеження доступу.

У цьому контексті керівні документи, що визначають віднесення інформації до певного рівня обмеження доступу, сфокусовані на наявність

певного обсягу інформації конкретний момент часу та на конкретному носії інформації. Тут варто зауважити, що ІТС не є повними аналогами матеріальних носіїв секретної інформації, як визначено в Законі України «Про державну таємницю» від 21 січня 1994 року № 3855-XII [8]. Відмінність полягає у постійній модифікації інформації, зміни її кількості та міграції серед вузлів ІТС.

Розглянемо можливість витоку інформації через приховані канали витоку інформації через незахищений вузол ІТС (на рисунку 2 позначений node 1).

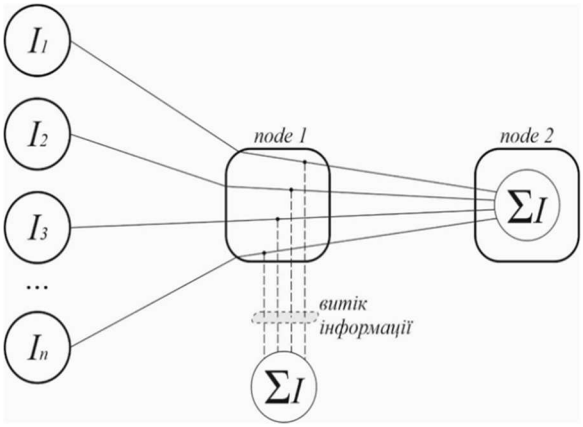

Рис. 2. Варіант витоку інформації через незахищений вузол ІТС

Типова побудова телекомунікаційної мережі передбачає наявність шлюзового вузла, через який проходить вся інформація, що стосується функціонування ІТС, які розгортаються на базі цієї мережі. Припустимо, що інформація, яка циркулює в ІТС, що нами аналізується, не має обмеження доступу. Відповідно до вимог Постанови КМУ від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [6], наявність засобів технічного захисту інформації, зокрема, забезпечення такої властивості як «конфіденційність», не є обов'язковою. У цьому випадку можливий витік інформації, який дозволить зловмисникам отримати за певний час інформацію, що призначена для вузла node 2. З метою недопущення витоку інформації необхідно застосовувати добре розроблені та апробовані підходи до захисту інформації на вузлах мережі які не обробляють інформацію з обмеженим доступом.

Розглянемо інший варіант, який можливий в інтранет-мережі прикордонного відомства. Державна прикордонна служба України поступово переходить на систему електронного документообігу [9]. Починаючи з 2020 року документообіг Держприкордонслужби стає електронним, що передбачає зберігання електронних документів на серверах системи електронного документообігу. У цьому контексті варто зауважити, що в цій системі циркулюють тільки документи, що не мають грифу обмеження доступу, що, в свою чергу, передбачає відсутність здійснення певних заходів (створення комплексної системи захисту інформації) на вузлах системи та й для системи в цілому.

Припустимо, що вузли системи (node 1 … node n) надсилають k-му вузлу відкриту частину агрегованої інформації в різні моменти часу (рисунок 3).

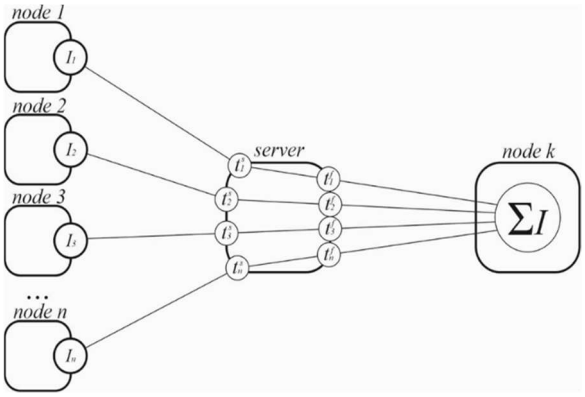

Рис. 3. Проходження інформації через сервер системи

Зазначена інформація надходить на сервер системи в моменти часу i_i^s та зберігається на ньому до моменту часу i_i^f (де i – індекс вузла). Відкладемо на часовій діаграмі періоди знаходження складових агрегованої інформації $\sum I$. Як видно з рисунка 4, можливе існування такого періоду часу, в якому на сервері міститься вся агрегована інформація $\sum I$.

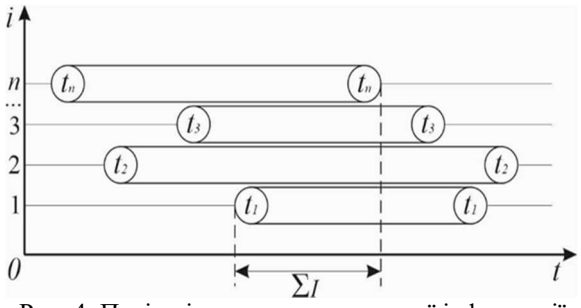

Рис. 4. Період існування агрегованої інформації

Вищенаведене дозволяє стверджувати про можливість знаходження інформації з вищим ступенем обмеження доступу на вузлі ІТС, чим це передбачено наявними дозволами та вимогами.

Аналіз існуючих моделей розмежування доступу показав відсутність врахування в них такого поняття як «агрегована» інформація, що в свою чергу не дозволяє запобігти порушенню її конфіденційності. Вирішення цієї проблеми можливе шляхом формування «агрегованого контейнеру», рівень доступу до якого визначається залежно до його заповнення необхідною інформацією. З метою формалізації цього процесу введемо поняття тематичного класифікатора агрегованого об'єкта, як сукупність підмножин нижчого рівня $\left\{T^Z\right\} = \left\{\tau_1^Z, \tau_1^Z, ..., \tau_n^Z\right\}$, де z – індекс

агрегованого об'єкту, n – кількість складових агрегованого об'єкту, яку визначає виконавець. Кожній складовій тематичного класифікатора та елементам підмножини визначається відповідний рівень конфіденційності, а саме відображення на множину рівнів конфіденційності $F : T^Z \to L, \tau_i^Z \to L$. Аналіз керівних документів показав, що складові z-го об'єкта мають однаковий рівень конфіденційності, але в загальному випадку це не є обов'язковим.

Введемо поняття «статус агрегованого контейнеру», таких статусів повинно бути два «доступний» та «критичний». Статус «агрегованого контейнеру» «доступний» присвоюється за наявності ступеня наповненості менше *n-1*. При досягненні заповнення «агрегованого контейнеру» до стану *n-1* його статус визначається як «критичний». Протокол роботи системи з такого типу контейнерами наведено на рисунку 5.

Загальний алгоритм протоколу обміну наступний, при статусі «доступний» заповнення контейнеру здійснюється без обмежень доступу до нього. У випадку переходу контейнера у статус «критичний» вузол, який ініціює заповнення контейнера, інформується про статус контейнера і передає дані на захищений вузол. В цей час, на захищений вузол сервер передає «агрегований контейнер» зі статусом «критичний». В результаті виконання цієї процедури всі вузли ІТС не порушують вимог керівних документів із захисту інформації, а інформація формується та зберігається на захищених вузлах системи.

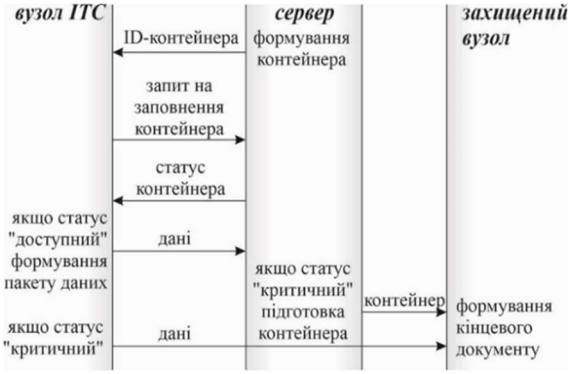

Рис. 5. Узагальнений протокол обміну інформації між вузлами ІТС

Висновки та перспективи подальших досліджень

Аналіз нормативних документів із класифікації інформації з обмеженим доступом показав, що існуючі моделі розмежування доступу не передбачають наявність «агрегованої» інформації, рівень обмеження доступу якої зростає залежно від її кількості. Визначені можливі канали прихованого витоку інформації без порушення політики безпеки інформаційно-телекомунікаційної системи. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження нового протоколу обміну між вузлами ІТС. Напрямами подальших досліджень є деталізація взаємодії між захищеними та незахищеними вузлами мережі.

Література

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено Наказом департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від "28" квітня 1999 р. № 22. Із змінами згідно наказу адміністрації Держспецзв'язку від 28.12.2012 № 806. **2. Bell D. E.** Unified Exposition and Multics Interpretation MITRE Corporation / D.E. Bell, L.J. LaPadula // Secure Computer System: (1976). [Электрон. ресурс]. – Режим доступа к ресурсу: http://csrc.nist.gov/ publications/history/bell76.pdf. **3. Biba K.** Integrity Considerations for Secure Computer Systems / K. Biba // Technical Report MTR-3153, MITRE Corporation, Bedford, MA (Apr. 1977). **4. Семенов С. Г.** Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі / С. Г. Семенов, В. М. Зміївська, А. В. Голубенко // Системи обробки інформації – 2015. – № 3. – С. 99-102. **5.** Наказ Служби безпеки України від 23.12.2020 № 383. Зареєстровано в Міністерстві юстиції України 14 січня 2021 р. за № 52/35674 «Про затвердження Зводу відомостей, що становлять державну таємницю» https://zakon.rada.gov.ua/laws/show/z0052-21#n7 **6.** Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». **7.** Наказ Адміністрації Державної прикордонної служби України від «07» липня 2011 року № 501 «Про затвердження Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України та Інструкції із захисту публічної інформації у Державній прикордонній службі України» (з доповненнями). **8.** Закон України "Про державну таємницю" від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93. https://zakon.rada.gov.ua/laws/show/3855-12 **9.** Наказ АДПСУ від 08.12.2020 року № 522аг «Про введення в експлуатацію системи електронного документообігу ДПСУ».

PROTOCOLS FOR THE EXCHANGE OF "AGGREGATED" INFORMATION IN THE INFORMATION AND TELECOMMUNICATION SYSTEM

Mykhailo Strelbitskyi *(doctor of Engineering, professor)*
Valentyn Mazur *(doctor of military sciences, professor)*
Volodymyr Lemeshko *(candidate of military sciences, docent)*

Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi city, Ukraine

In the article, based on the classification of information with limited access, the prerequisites for violation of its confidentiality were determined in compliance with the requirements of the security policy of the information and telecommunications system. It was determined that an increase in the amount of information can lead to an increase in the level of access restriction. Sets of information of this type are defined as "aggregated". The conditions for violation of information security, the level of confidentiality of which depends on its quantity, were given. Possible channels of hidden leakage of information from network nodes without violating the security policy of the information and telecommunications system were identified. A method of preventing unauthorized access of information system subjects by introducing a new exchange protocol between nodes of information and telecommunication systems was proposed. The developed protocol for the exchange of "aggregated" information between network nodes provides for the use of an "aggregated" information container, which ensures the formation of information with a higher level of access on a protected node of the information and telecommunications system.

Keywords: *information, confidentiality, protocol, information system.*

References

1. Criteria for evaluating the security of information in computer systems against unauthorized access. [Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu] ND TZI 2.5-004-99. Approved by the Order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22. Amended in accordance with the Order of the State Special Communications Administration No. 806 dated December 28, 2012. **2.** Bell, D. E., LaPadula, L.J. (1976). Unified Exposition and Multics Interpretation MITRE Corporation. *Secure Computer System*, available at: http://csrc.nist.gov/publications/history/bell76.pdf. **3.** Biba K. (1976). Integrity Considerations for Secure Computer Systems, Technical Report MTR-3153, MITRE Corporation, Bedford, MA. **4.** Semenov S. H., Zmiivska V.M., Holubenko A.V. (2015). Comparative studies of access control technologies for data protection in a computer system. [Comparative studies of access control technologies for data protection in a computer system], Information processing systems , No 3, pp 99-102. **5.** On the approval of the Compendium of information constituting a state secret. [Pro zatverdzhennia Zvodu vidomostei, shcho stanovliat derzhavnu taiemnytsiu] (2021). Order of the Security Service of Ukraine dated 12/23/2020 No. 383. Registered with the Ministry of Justice of Ukraine on January 14, 2021 under No. 52/35674, available at: https://zakon.rada.gov.ua/laws/show/z0052-21#n7 **6.** On the approval of the Rules for ensuring the protection of information in information, electronic communication and information and communication systems . [Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh], (2006). Resolution of the Cabinet of Ministers of Ukraine dated March 29, 2006 No. 373 **7.** On the approval of the List of information constituting official information in the State Border Service of Ukraine and the Instructions for the protection of public information in the State Border Service of Ukraine" (with additions). [Pro zatverdzhennia Pereliku vidomostei, shcho stanovliat sluzhbovu informatsiiu u Derzhavnii prykordonnii sluzhbi Ukrainy ta Instruktsii iz zakhystu publichnoi informatsii u Derzhavnii prykordonnii sluzhbi Ukrainy» (z dopovnenniamy)], (2011). Order of the Administration of the State Border Service of Ukraine dated July 7, 2011 No. 501 **8.** Law of Ukraine "On State Secrets" [Zakon Ukrainy "Pro derzhavnu taiemnytsiu] (1994). available at: https://zakon.rada.gov.ua/laws/show/3855-12 **9.** On putting into operation the system of electronic document circulation of the DPSU. [Pro vvedennia v ekspluatatsiiu systemy elektronnoho dokumentoobihu DPSU] (2020). Order of the Administration of the SBGSU dated 08.12.2020 No. 522ah.