УДК 004.75
DOI: 10.31891/2219-9365-2021-68-2-7

СТЕЦЮК М. В.
Хмельницький національний університет

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ ПРИ ВПЛИВАХ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В роботі проведено аналіз використання інформаційних систем (ІС) різного призначення, яке продовжує стрімко зростати. Зловмисники прагнуть отримати певні фінансові вигоди і це спонукає їх до розробки зловмисного програмного забезпечення (ЗПЗ), яке використовують проти ІС. Тому, актуальними на сьогодні завданнями є розробка спеціалізованих ІТ різного призначення, які б забезпечували можливості з захисту інформації в умовах впливів ЗПЗ та комп'ютерних атак.

Результатами роботи є створення інтегрованих в апаратні та програмні компоненти ІС засобів захисту інформації ІС, які у своїй сукупності утворюють комплексну підсистему захисту інформації: сегментування мережі, виокремлення серверної частини в окрему під мережу з можливістю гнучкого налаштування політик безпеки для кожного сегмента підвищує стійкість ІС до атак ЗПЗ; застосування криптографічних засобів захисту гарантує відсутність несанкціонованого доступу до інформації в фізично неконтрольованих каналах передачі інформації, а також зменшує можливості ведення розвідки комп'ютерної мережі ІС; застосований метод запуску клієнтських АРМ з двохфакторною автентифікацією ПЗ та користувача унеможливлює підключення нелегальних програм та незареєстрованих копій штатного ПЗ; нетривіальні процедури контролю за операціями маніпулювання даними, виконання всіх операцій з даними під управлінням транзакцій гарантують цілісність та узгодженість інформації в ІС, а застосування контролю активності АРМ, гнучка дворівнева система управління наданням прав доступу до ресурсів ІС додатково зменшує вірогідність несанкціонованого доступу до інформації; автоматизована система резервного копіювання з територіальним розмежуванням місць зберігання копій та перевіркою їх робото здатності унеможливлює не відновлювану втрату інформації.

Проведені експерименти підтверджують працездатність засобів захисту інформації ІС та зроблені висновки. Реакція ІС на впливи, змодельовані в обох експериментах була очікуваною і в межах встановлених часових меж.

Розроблений метод забезпечення захисту інформації ІС в поєднані із організаційно-правовими заходами, використані як єдиний комплекс, дозволяє отримати технологію, застосування якої при розробці спеціалізованої ІС, гарантує високий рівень її захищеності її ресурсів від деструктивних впливів.

Ключові слова: інформаційні системи, захист інформації, ефективність, метод забезпечення захисту інформації.

M. STETSYUK
Khmelnitskyt National University

METHOD OF ENSURING PROTECTION OF INFORMATION IN SPECIALIZED INFORMATION TECHNOLOGIES UNDER THE INFLUENCE OF MALICIOUS SOFTWARE

The paper analyzes the use of information systems (IS) for various purposes, which continues to grow rapidly. Attackers seek financial gain, and this encourages them to develop malicious software, which they use against IP. Therefore, the urgent task today is to develop specialized IT for various purposes, which would provide opportunities to protect information in the face of SDR and computer attacks.

The results of the work are the creation of integrated into the hardware and software components of IP information security, which together form a comprehensive information security subsystem: network segmentation, separation of the server part into a separate network with the ability to flexibly configure security policies for each segment. ЗПЗ; the use of cryptographic means of protection ensures the absence of unauthorized access to information in physically uncontrolled channels of information transmission, as well as reduces the ability to conduct intelligence of the computer network IP; the applied method of running client workstations with two-factor authentication of software and user makes it impossible to connect illegal programs and unregistered copies of regular software; non-trivial procedures for control over data manipulation operations, execution of all data operations under transaction management guarantee the integrity and consistency of information in the IS, and the use of workstation activity control, flexible two-tier system for managing access to IP resources further reduces the likelihood of unauthorized access to information; automated backup system with territorial delimitation of places of storage of copies and check of their working ability prevents non-recoverable loss of information.

The conducted experiments confirm the efficiency of IP information protection means and the conclusions are made. The response of the IP to the effects simulated in both experiments was expected and within the established time limits.

The developed method of protection of IP information in combination with organizational and legal measures used as a single complex, allows to obtain technology, the use of which in the development of specialized IP, guarantees a high level of protection of its resources from destructive influences.

Keywords: information systems, information protection, efficiency, method of information protection.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Використання інформаційних систем (ІС) різного призначення продовжує стрімко зростати. Зловмисники прагнуть отримати певні фінансові вигоди і це спонукає їх до розробки зловмисного

програмного забезпечення (ЗПЗ), яке використовують проти ІС. Тому, актуальними на сьогодні завданнями є розробка спеціалізованих ІТ різного призначення, які б забезпечували можливості з відмовостійкості, живучості та захисту інформації в умовах впливів ЗПЗ та комп'ютерних атак.

Розглянемо види загроз інформації, що обробляється в спеціалізованій ІС.

Питання забезпечення захисту інформації є фундаментальною складовою, поряд із відмовостійкістю та живучістю, при розробці інформаційної технології для побудови на її основі спеціалізованих інформаційних систем, що працюють в умовах впливів зловмисного ПЗ. Серед загроз, з якими можуть зіткнутися інформаційні системи, можна виділити наступні [1-5]:

1. Зловмисне програмне забезпечення. Його деструктивні дії можуть зробити недоступними функції спеціалізованої інформаційної системи, або окремих її робочих місць.

2. Отримання несанкціонованого доступу до інформації. Може призвести до втрати конфіденційності інформації, або (та) навмисного її спотворення, знищення.

3. Ненавмисне спотворення інформації в результаті некваліфікованих дій клієнтів інформаційної системи.

Рис. 1. Методи забезпечення захисту інформації в ІС

Щоб зменшити ризики від впливу перелічених вище негативних факторів, необхідно розбудовувати систему захисту інформації в ІС з урахуванням всіх відомих методів захисту [6-9] (рис. 1). Планування системи захисту інформації в спеціалізованій ІТ, розпочинається на етапі розробки технічного завдання на її проектування, а сам проект повинен базуватись на певній моделі. Оскільки забезпечення захисту інформації є постійний процес в життєвому циклі інформаційної системи, то його забезпечення повинно базуватись на системному підході, який повинен гарантувати деякий поріг, що не знижується з плином часу. Це пов'язано з тим, що спеціалізовані інформаційні системи характеризуються тривалим часом їх використання, який обчислюється десятками років. За цей час зловмисне ПЗ може зробити крок у своєму розвитку, що може призвести до подолання системи захисту.

Структурно вона повинна включати кілька рівнів, кожен із яких має створювати певний бар'єр протидії зловмисному ПЗ, доступу до інформації сторонніх осіб та необережному поводженню із інформацією користувачами системи. При цьому створювана системи захисту інформації ІС [10-12] повинна забезпечувати виконання найбільш важливих правил свого функціонування:

1. Доступність - можливість швидкого отримання потрібної інформацію легальними користувачами.

2. Цілісність - актуальність та захищеність інформаційних даних від несанкціонованих змін.

3. Конфіденційність - неможливість несанкціонованого доступу до даних.

У відповідності до проголошених правил було виконано побудову підсистеми забезпечення захисту інформації для спеціалізованої ІС.

Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз представлено в роботі [10].

Таким чином, розробка спеціалізованих ІТ різного призначення, які б забезпечували можливості з захисту інформації в умовах впливів ЗПЗ та комп'ютерних атак є актуальною.

Метод забезпечення захисту інформації спеціалізованих ІТ

Проведений аналіз [1]-[12] показав, що на сьогодні основна загроза для інформації, що зберігається в комп'ютерній системі, надходить із глобальної комп'ютерної мережі. Тому, структура комп'ютерної мережі, на якій буде базуватись робота ІС повинна передбачати її розділення на локальні сегменти з обмеженням доступу до них. В таких захищених сегментах із контрольованим доступом, розміщуються серверна частина ІС та її клієнтські місця, що забезпечують основну функціональність системи.

Такий підхід до побудови комп'ютерної мережі дозволив зменшити ризик для ІС з боку зловмисного ПЗ та спроб несанкціонованого доступу до інформаційної системи з використанням каналів INTERNET.

ISSN 2219-9365

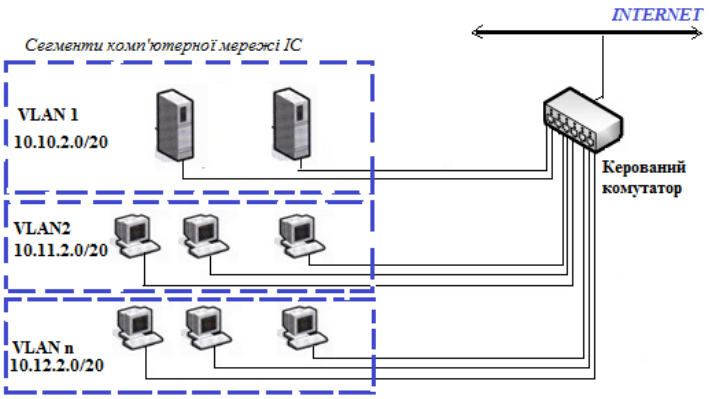

Рис. 2. Спрощена топологія сегментованої комп'ютерної мережі спеціалізованої ІС

Застосування керованого комутатора з функцією створення віртуальних комп'ютерних мереж (VLAN) дозволило отримати можливість:

1. Захистити мережу від стороннього втручання. Порт керованого мережевого комутатора зможе ігнорувати та відсікати пакети, які надходять з інших підмереж, причому незалежно від початкової IP-адреси.

2. Гнучко управляти розділенням комп'ютерів по віртуальним підмережах, забезпечуючи ізольованість одна від одної, при цьому їх топологія не залежить від того, де фізично знаходяться мережі компоненти.

3. Забезпечення зменшення широкомовного трафіку в мережі. Кожна створена віртуальна підмережа є окремим широкомовним доменом, широкомовний трафік якого не транслюватиметься між різними підмережами, зменшуючи навантаження на мережеве обладнання.

4. Розбиття мережі на віртуальні підмережі, дозволило застосовувати свої правила безпеки для кожної із них (рис.3), що загалом підвищує безпеку та керованість мережі в цілому.

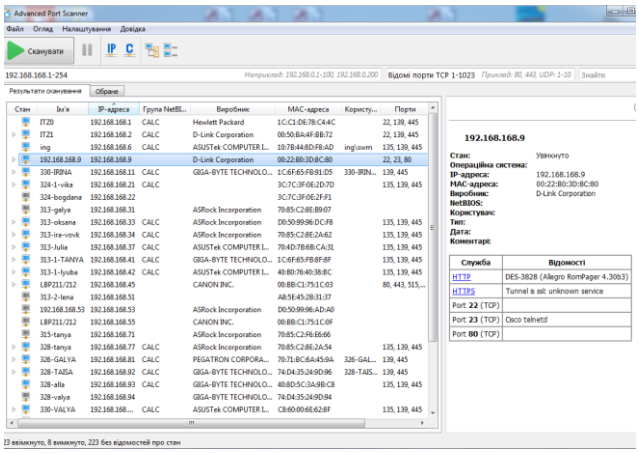

Рис. 3. Налаштування політик безпеки компонентів мережі ІС.

Це дозволяє гнучко налаштувати фільтрацію пакетів для кожної підмережі, яка виконується з оцінкою даних на основі IP-інформації, що міститься в заголовку пакета, а саме адреси відправника і одержувача пакета. В процесі фільтрації пакетів інформація, отримана з IP-заголовку зіставляється зі списком правил фільтрації для дозволу або заборони передачі пакета. В розробленій ієрархії правил фільтрації враховуються наявні поля IP-адрес, типи протоколів, номери портів відправника і одержувача. Перш ніж дозволити пакету продовження передбачуваного для нього маршруту, правила фільтрів пакетів перевіряють вказані в них дані на відповідність зумовленим значенням. Це дозволяє, зберігаючи високий рівень захисту інформації в мережі, мати гнучко керований доступ до її ресурсів та різко скоротити об'єм інформації про мережу, яку отримає зловмисник при спробі її розвідки, особливо враховуючи ту обставину, що вміст пакетів має криптографічний захист.

Окрім базування ІС на сегментовану комп'ютерну мережу, передбачається протидія зловмисному ПЗ на рівні окремої комп'ютерної системи, на якій буде базуватись клієнтське робоче місце.

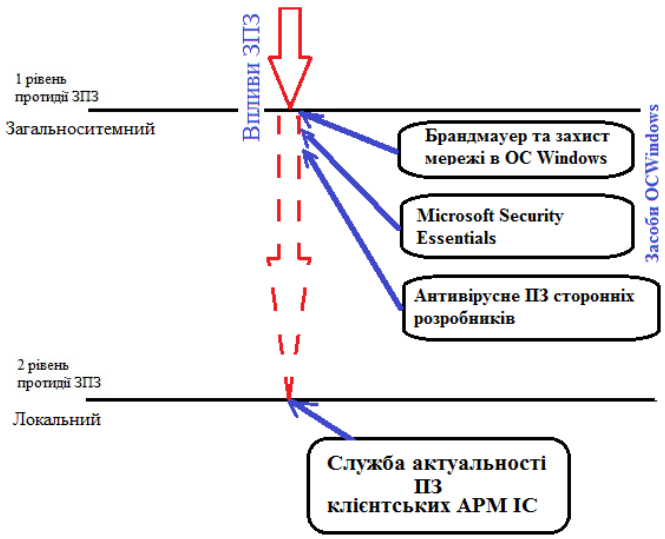

Рис. 4. Модель організації дворівневої схеми протидії ЗПЗ для клієнтських АРМ ІС

Ця протидія буде здійснюється на двох рівнях - як на загальносистемному із використанням можливостей операційної системи, так і локальному, із використанням ресурсів самої ІС (рис. 4). Загальносистемний рівень є основним в протидії ЗПЗ. На ньому, як видно з рис. 4, використовуються найпотужніші засоби протидії. Але все одно це не дає повної гарантії безпеки. Тому, локальна протидія ЗПЗ засобами самої ІС, особливо з можливістю самовідновлення пошкодженого ПЗ, дозволяє повернути клієнтському АРМ робото здатність навіть в умовах, коли комп'ютер знаходиться під контролем ЗПЗ.

Для цього в рамках ІС залучається ПЗ служби контроля актуальності програмного забезпечення клієнтських АРМ ІС. Її основне призначення - автоматичне оновлення версій програмного забезпечення АРМ. Але аналіз її алгоритму роботи показав, що служба контролю актуальності ПЗ АРМ може бути використана і для протидії ЗПЗ.

Вона не зможе виявляти і знешкоджувати зловмисні програми, але відповідно до свого алгоритму роботи, вона може локально ліквідовувати їх прояви, такі як знищення програмних модулів АРМ, їх пошкодження, шифрування і таким чином посилювати захист інформації ІС, відновлювати доступ до її функцій.

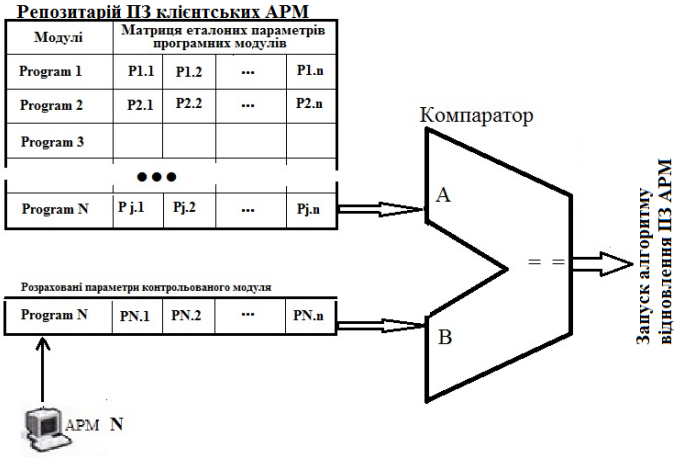

Рис. 5. Архітектура служби контролю актуальності ПЗ клієнтських АРМ

Як видно з рис. 5, в основі служби контроля актуальності ПЗ лежить процедура програмного компаратора, яка виконується як фоновий процес. Її алгоритм та схема роботи зображені на рис. 6.

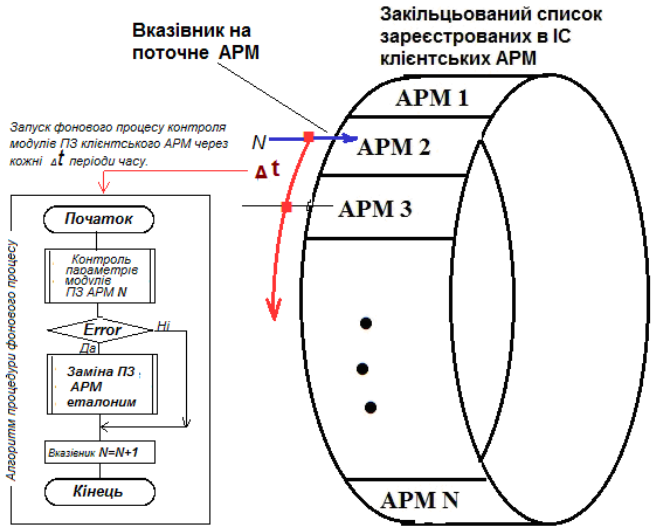

Рис. 6. Схема та алгоритм контролю актуальності ПЗ клієнтських АРМ

Його задача - здійснення із заданим періодом Δt перевірку параметрів модулів ПЗ клієнтських АРМ з еталоними, що зберігаються в репозитарії служби. Якщо в ході перевірки модуль не буде знайдено в місці свого призначення, або його параметри будуть відрізнятись від еталоних, то він буде визнаний як неактуальний. Це призведе до запуску процедури, яка виконає заміщення програмного модуля еталоним із репозитарію модулів. При цьому причина пошкодження або знищення модуля неважливі - основна мета відновлення функціональності АРМ і, таким чином, недопущення блокування доступу до інформації, її втрати, спотворення або пошкодження, при функціонувані неактуального або пошкодженого ПЗ АРМ з можливим відхиленням від заданих алгоритмів.

Несанкціонований доступ до даних інформаційної системи можна отримати шляхом фільтрації та наступного аналізу її мережевого трафіка, у випадку наявності фізичного доступу до інформаційних каналів системи. Для унеможливлення або утруднення доступу до даних таким шляхом, застосовано криптографічний захист інформації.

Крім того, інформаційні канали окремих сегментів комп'ютерної мережі, наприклад, її ядра, до якого входять серверна група та основні клієнтські місця, виконані таким чином, що унеможливлюють фізичний доступ до них зловмисників (рис. 11). В таких сегментах можна вести обмін даними інформаційної системи між її складовими без втрати часу на криптографічний захист, що дозволяє отримати максимальну продуктивність роботи системи.

Наступним шляхом отримання несанкціонованого доступу до даних інформаційної системи може бути використання несанкціонованого підключення до інформаційної системи. Для цього зловмисник може спробувати скористатись як штатним програмним забезпеченням так і власноруч розробленим. Щоб перекрити такий шлях доступу до даних інформаційної системи, ведеться реєстрація всіх екземплярів клієнтського програмного забезпечення та їх параметрів запуску (IP-адреса комп'ютерної системи, дискові шляхи, імена файлів програм і т. і.). Крім цього використовується спеціальний алгоритм їх запуску (рис. 7) який передбачає двофакторну перевірку легитимності екземпляра програми.

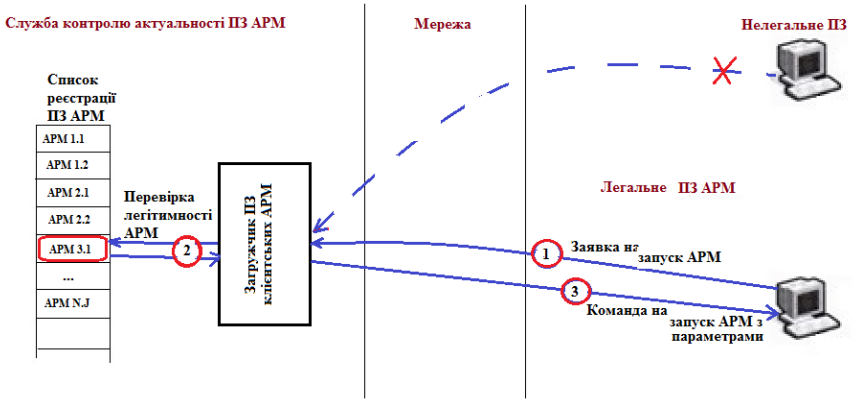

Рис. 7. Схема двохфакторної перевірки легітимності ПЗ АРМ

Його особливість в тому, що оператор АРМ сам не може запустити програмну систему свого АРМ, через те, що йому невідомі параматри запуску та з'єднання, окрім тих, що ідентифікують його самого. Він лише подає заявку на запуск програмі загружчику, яка входить до складу служби контролю актуальності ПЗ АРМ (позиція 1 рис. 7). Завантажувальник отримавши заявку від деякого АРМ перевіряє наявність його реєстрації в ІС (позиція 2 рис. 7). Якщо реєстрація підтверджується, то виконує віддалений запуск ПЗ клієнтського АРМ на комп'ютері, де згідно реєстрації має функціонувати АРМ, що подало заявку на запуск і тільки з тими параметрами, що зберігаються в репозитарії ПЗ служби контролю актуальності клієнтського ПЗ (позиція 3 рис. 7). В процесі запуску оператор, що подав заявку на запуск, вводить свої реєстраційні дані, ідентифікує себе в ІС, проходячи автентифікацію. Таким чином, унеможливлюється підключення незареєстрованих екземплярів програм та гарантується доступ до інформації тільки легальним користувачам. Ця робота покладена на службу контролю актуальності програмного забезпечення клієнтських робочих місць.

Питання контрольованого доступу до ПЗ клієнтських АРМ є важливим в переліку заходів забезпечення інформаційної безпеки - це самий простий шлях для зловмисника подолати систему захисту ІС. Тому, саме для цієї ланки системи захисту інформації є важливим дотримання персоналом АРМ організаційно-правових заходів безпеки.

Гіпотетично є два шляхи доступу для отримання доступу до ПЗ клієнтського АРМ - зовнішній та внутрішній. Зовнішній шлях полягає в отримані віддаленого контролю над комп'ютером, на якому встановлене ПЗ клієнтського АРМ ІС. Оскільки ПЗ АРМ включає в себе алгоритми ідентифікації легітимності користувача, то спроба його віддаленого запуску не буде досить простою. Особливо, коли кількість спроб підключення обмежена і отримати пароль шляхом перебору є практично неможливим.

Зловмисник може діяти не тільки зовні, але і зсередини системи, якщо йому вдасться подолати організаційно-правові заходи безпеки. З метою не допуску такого розвитку ситуації, коли зловмисник отримає доступ до легального ПЗ клієнтського робочого місця, в нього включена функція контролю за активністю його оператора.

Вона реалізована як фоновий процес, який циклічно контролює активність оператора відповідно до алгоритму, наведеному на рис. 8. Як видно з нього, фоновий процес взаємодіє із будь якою функцією ПЗ, запущеною оператором АРМ.

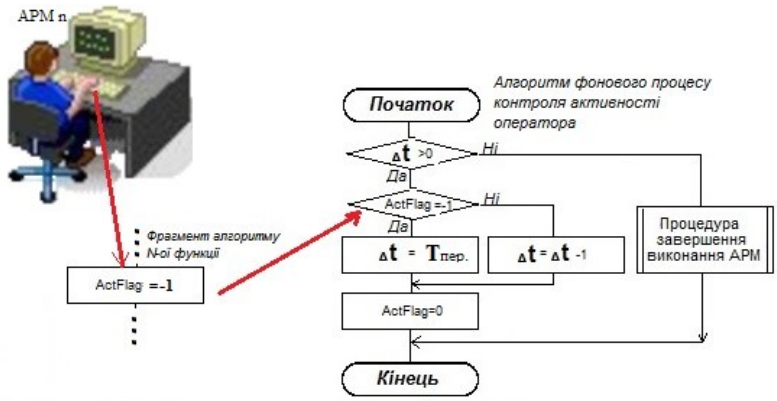

Рис. 8. Схема взаємодії програмних модулів клієнтських АРМ по контролю за активністю оператора

У випадку відсутності активності оператора АРМ на встановленому проміжку часу, фоновий процес запустить процедуру завершення роботи ПЗ клієнтського робочого місця.

Кожен клієнт ІС при реєстрації його, як користувача ІС, не отримує ніяких прав на інформаційні ресурси системи. Всі необхідні права, для управління даними в такій системі надаються ролі (прообразу посади). Клієнту ж надається право виконувати певну роль в інформаційній системі. Цей підхід дозволяє уникнути проблеми залишкових прав, коли функції клієнта в системі з часом змінюються, а деякі права доступу до ресурсів інформаційної системи залишаються. Запропонований підхід передбачає зміну ролі користувача в ІС, гарантуючи при цьому, що права по старій ролі будуть ним втрачені, а по новій набуті. Таким чином реалізується перший рівень управління доступом до ресурсів ІС в запропонованій технології реалізації спеціалізованих ІС. Як правило, він реалізується з використанням штатних засобів системи адміністрування ІС.

З метою покращення гнучкості управління правами на інформаційні ресурси, та з метою збільшення швидкості реакції на різні деструктивні прояви в ІС, дана технологія побудови ІС передбачає введення ще одного рівня управління правами доступу до її інформаційних ресурсів.

На цьому рівні розмежування прав виконується на рівні клієнтського робочого місця. Це дозволяє

оперативно реагувати на події в ІС шляхом заборони роботи деяких робочих місць, або переключення їх в режим, що не передбачає внесення змін в дані. При цьому робота інших клієнтських робочих місць ніяк не порушується.

Реалізація другого рівня управління правами доступу до ресурсів ІС стала можливою, завдяки наявності реєстрації всіх екземплярів клієнтського програмного забезпечення в її БД, як це описано вище. Його особливістю є те, що він становить базову фундаментальну частину ПЗ клієнтського робочого місця, яка є типовою для всіх робочих місць в запропонованій технології. Алгоритм управління правами на рівні робочого місця допускає зміну прав зі сторони адміністратора системи у будь який час, а сама ця зміна буде врахована при спробі виконати наступну операцію над даними.

Дворівнева система управління доступом до даних спеціалізованої ІС дозволяє значно зменшити ризик випадкового спотворення даних зі сторони операторів клієнтських робочих місць, через випадкове набуття прав. Але залишається можливість їх спотворення в процесі виконання легальних операцій з даними згідно своєї ролі у системі.

ІС в плані інформаційної безпеки повинна відповідати трьом безпековим принципам [1]: конфіденційності, цілістності та доступності інформації. При вирішенні задачі захисту інформації від несанкціонованого копіювання необхідно забезпечити виконання одночасно двом із них - конфіденційносі та доступності.

Аналіз місць вразливості ІС щодо можливості несанкціонованого копіювання показав, що це в принципі неможливо з клієнтського робочого місця, оскільки самі АРМи побудовані з урахуванням правил моделі безпеки Кларка-Вільсона, згідно яких оператор (суб'єкт) не має прямого доступу до даних і відповідно, навіть у випадку коли зловмисник знаходиться всередині системи, він гарантовано позбавлений можливості несанкціонованого копіювання інформації.

І тільки в випадку отримання прямого доступу зловмисником до БД або її копій це стане можливим. Оскільки БД та її копії розміщуються на комп'ютерах серверної групи, відносно яких діють самі жорсткі заходи захисту інформації від організаційно-правових до фізичних, то така ситуація є маловірогідною, незважаючи на територіальне рознесення комп'ютерів цієї групи.

Щоб максимально зменшити вірогідність спотворення інформації в результаті некваліфікованих дій клієнтів інформаційної системи, започаткована наступна організація їх роботи.

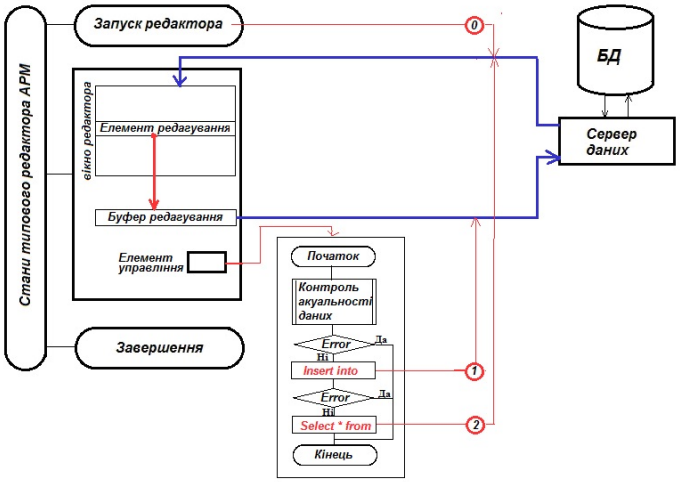

Рис. 9. Схема контролю ПЗ клієнтського АРМ за діями оператора

Щоб максимально унеможливити їх спотворення в процесі функціональної діяльності, технологія розробки ПЗ клієнтських робочих місць, де виконуються операції редагування даних передбачає включення до його складу типових редакторів даних, які включають в себе модулі контролю, які перешкоджають внесенню в БД неузгоджених даних. До його складу включені процедури програмного контролю правильності введених даних, їх несуперечливості раніше введеним. Такий підхід підвищує ступінь актуальності даних, поміщених в базу даних, відхиляє технічні помилки. Схема організації роботи такої структури показана на рис. 9.

Її особливістю є те, що маніпулювання критичними даними з точки зору їх цілістності, зі сторони оператора клієнтського АРМ, знаходиться під програмним контролем.

Як видно з рис. 9, обрані для редагування оператором елементи даних поміщаються в спеціальний буфер, в якому і здійснюється їх редагування. Після закінчення цієї операції оператор робить спробу зберегти зміни. Але перед їх відправкою на сервер БД нові значення елементів даних перевіряються на непротиріччя та цілісність. Якщо перевірка дасть позитивний результат, то дані відправляються на сервер БД, інакше в їх

збережені буде відмовлено. Такий підхід дозволяє в великій мірі уникнути випадкового, ненавмисного спотворення інформації ІС зі сторони операторів клієнтських робочих місць.

Робота підсистеми транзакцій побудована з урахуванням правил абстрактної моделі захисту інформації Кларка-Вільсона (Clark-Wilson) яка біла оприлюднена 1987 році. Вважається однією з найдосконаліших у відношенні підтримки цілісності інформаційних систем. Дана модель заснована на повсюдному використанні транзакцій і ретельному оформленні прав доступу суб'єктів до об'єктів.

Особливістю цієї моделі є розповсюдження системи захисту на третю сторону - на програму (транзакцію). Модель побудована на тристоронніх відносинах суб'єкт-програма-об'єкт (де програма взаємозамінна з транзакцією). В рамках цих відносин суб'єкт немає прямого доступу до об'єкта. Доступ до об'єкта можливий лише через програму (транзакцію).

Крім того, в моделі Кларка-Вільсона транзакції вперше були побудовані за методом верифікації, тобто ідентифікація суб'єкта проводилася не тільки перед виконанням команди від нього, але і повторно після виконання. Це дозволило зняти проблему підміни учасника в момент між його ідентифікацією і власне командою.

Схема роботи підсистеми транзакцій показана на рис. 10. Будь-які маніпуляції над інформацією в ІС охоплюються транзакцією. Її властивості гарантують, що в ході виконання транзакції вона або гарантовано приведе БД до нового несуперечливого стану у випадку її підтвердження, або поверне її до попереднього, з якого вона почалась у випадку її відкату.

Ця схема є складовою частиною типового елемента маніпулювання даними ІС показаного на рис. 9, який працює відповідно до правила моделі Кларка-Вільсона, яке, в свою чергу, проголошує принцип, що тільки процедура (програма) може змінювати інформацію в БД.

Така схема роботи клієнтських АРМ гарантує забезпечення цілісності та несуперечливості інформації та її захист в цілому.

Рис. 10. Схема роботи підсистеми транзакцій як частини системи захисту інформації

Одним із важливих вирішуваних завдань в системі забезпечення захисту інформації під час експлуатації ІС є організація роботи підсистеми резервного копіювання, адже навіть у найнадійнішій системі існує ризик втрати інформації, а особливо при її роботі в умовах впливів ЗПЗ. Для систем, що працюють в таких жорстких умовах наявність механізму швидкого відновлення втрачених даних є необхідністю.

Ключовими параметрами для планування побудови підсистеми резервного копіювання є:

- час, на протязі якого система має бути відновлена;
- часовий період, втрата даних на протязі якого є прийнятною.

Їх значення вибираються залежно від специфіки роботи ІС та критичності інформаційної системи і є компромісом між витратами на її функціонування та допустимими втратами інформації.

Загальний устрій системи резервного копіювання показаний на рис. 11. Як видно із схеми, сервером резервних копій слугує фізично інший комп'ютер, який територіально розмежований із основним сервером керування БД ІС.

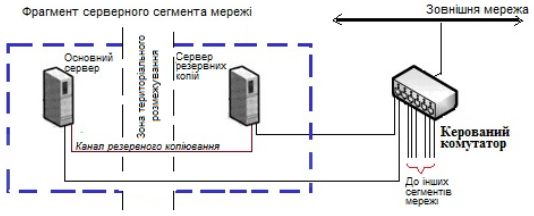

Рис. 11. Схема фрагмента комп'ютерної мережі підсистеми резервного копіювання

Такий вибір архітектури підсистеми резервного копіювання дозволив отримати стійку до різноманітних впливів, ІС в цілому. Ця схема практично унеможливлює одночасний вихід з ладу обох серверів і цим дає високі гарантії, що до збереження інформації, яка обробляється в системі.

Особливістю даної схеми є наявність окремого каналу резервного копіювання. Таке рішення дозволило позбутися вузького місця більшості систем резервного копіювання, пов'язаного із пропускною здатністю комп'ютерної мережі, забезпечивши максимальні швидкості передачі даних між серверами, як в режимі копіювання так і в режимі відновлення даних.

Ще однією особливістю організації роботи підсистеми резервного копіювання є розміщення

бібліотеки резервних копій на комп'ютері, який в ІС виконує функцію резервного сервера, що дозволяє, практично в режимі реального часу, перевірити працездатність отриманої копії БД.

Сам алгоритм резервного копіювання виконується в фоновому процесі відповідно до плану резервування, тому не потребує зупинки ІС, зрівнюючи дану ІС по цьому показнику із системами "високої доступності".

План резервування включає в себе процеси створення добових резервних копій, які додатково архівуються для зменшення займаного місця при їх зберіганні на диску. Також, створюються почасові, або з якимось іншим прийнятним періодом копії, які на протязі робочого дня і слугують джерелом даних резервного сервера. Ці копії для сервера створюються в режимі без використання компресії, але очисткою копії від видалених записів. Це дозволяє завжди мати готову для використання резервну копію БД, на яку перемкнеться резервний сервер у випадку аварії основного.

Для добових копій період зберігання встановлено три місяці, а для часових - три доби, після чого вони заміщаються більш актуальнішими, по мірі створення нових копій. Це дозволяє мати сталий об'єм бібліотеки резервних копій, уникаючи ситуації переповнення накопичувача.

Принцип конфіденційності, якому повинна відповідати система інформаційної безпеки, диктує вимогу забезпечення можливості отримання інформації лише легітимними користувачами.

Для безумовного виконання цього принципу в ІС для всіх АРМ було запроваджено систему криптографічного захисту, яка унеможливлює контроль мережевого трафіка обміну даними віддалених АРМ ІС із сервером БД. З цією метою використовується асиметрична криптосистема із парою ключів - відкритим ключем шифрування та закритим ключем для дешифрування (рис. 12).

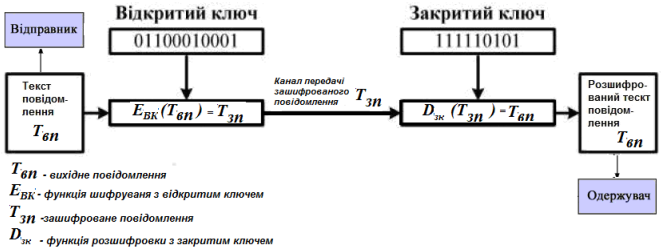

Рис. 12. Асиметрична криптосистема з відкритим ключем шифрування

Генерація таких пар ключів залежить від криптографічних алгоритмів, які ґрунтуються на односторонніх функціях. Для забезпечення безпеки передачі даних вимагається збереження таємниці закритого ключа, відкритий же ключ може відкрито розповсюджуватись без шкоди для безпеки.

Топологія комп'ютерної мережі, з використанням криптосистеми для передачі даних показана на рис. 13.

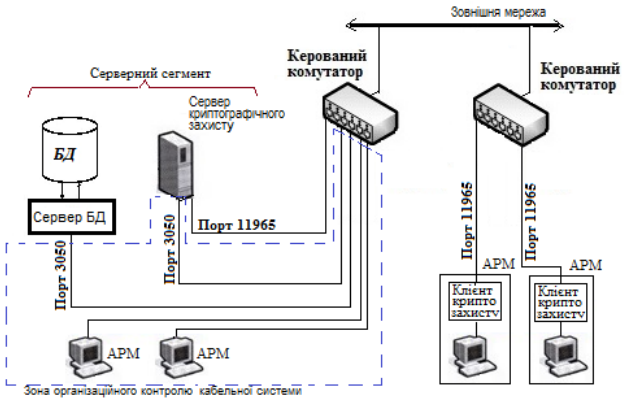

Рис. 13. Схема топології комп'ютерної мережі ІС із забезпеченням криптографічного захисту інформації

Зображена на рис. 13 схема комп'ютерної мережі включає до свого складу сервер криптографічного захисту. На нього покладається завдання створення шифрованих тунелів обміну даними між сервером БД та віддаленими клієнтськими АРМ ІС, кабельні та ефірні канали зв'язку з якими фізично не контролюються адміністраторами системи. Ті АРМ, що фізично знаходяться в зоні організаційного контролю кабельної системи, при обміні даними, засоби криптографічного захисту інформації не використовують, що збільшує продуктивність їх роботи і системи в цілому.

Клієнтські АРМ, які знаходяться поза цією зоною, обмін даними з сервером БД ведуть по захищеному каналу, загальна структура якого наведена на рис. 14.

Ініціатором встановлення з'єднання виступає віддалене АРМ. Сервер криптографічного захисту налаштований таким чином, що він постійно слухає свій порт, в даному випадку це порт 11965. При надходжені запиту на встановлення з'єднання від одного із віддалених АРМ ІС, сервер перевіряє його легітимність відповідно до параметрів налаштування таблиці зв'язків.

Якщо легітимність клієнта підтверджується, то сервер встановлює захищене з'єднання у вигляді шифрованого тунелю (рис. 14) із стискуванням даних, при їх передачі з використанням TCP і/або UDP протоколів. Застосування функції стискування даних дозволило підвищити пропускну здатність мережі.

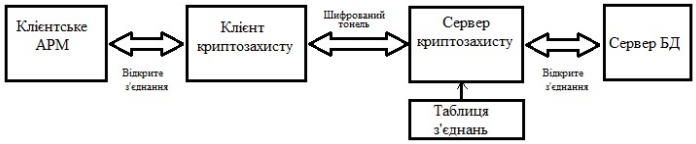

Рис. 14. Загальна схема шифрованого каналу передачі даних сервером БД та клієнтським АРМ ІС

При цьому знімається загроза зі сторони 'sniffer'-ів (переглядачів пакетів). Шифрування пакетів йде з самого початку, тому дані з'єднання (username та інші) разом з шляхом та ім'ям бази даних буде зашифровано, що значно ускладнює роботу потенційного зловмисника.

Як відомо, для успішної атаки на комп'ютерну мережу і ІС, що на неї базується, зловмиснику спочатку треба її вивчити, ведучи розвідку. Повне шифрування трафіка між клієнтським АРМ та сервером БД робить її практично невиконуваною задачею за прийнятний період часу, що в свою чергу не дозволить отримати службову інформацію, яка б дозволила почати атаку.

Проведено два експерименти, які демонструють ефективність роботи засобів захисту інформації в ІС. Перший експеримент полягав у перевірці реакції системи на відсутність активності оператора впродовж часу, що перевищує встановлений. Другий – перевірці реакції системи на спробу під'єднання до ІС нелегального ПЗ.

Для проведення першого експерименту було використано клієнтське АРМ №50. Змодельовано ситуацію відсутності активності оператора після його запуску. Результати експерименту наведені в табл.1 – подія 210547 та 210548 та в фрагменті log-файла (події 210547 та 210548), які зображені на рис.15.

File0023.log [vk.com]

210545	149	23.09.2021 8:05:10				192.168.168.1	192.168.168.16
210546	2	23.09.2021 8:09:25	23.09.2021 17:01:26			192.168.168.1	192.168.168.4
210547	50	23.09.2021 8:12:05	23.09.2021 8:40:01	1000	Stop ..... Timed Out	192.168.168.1	192.168.168.10
210548	50	23.09.2021 8:42:57	23.09.2021 9:21:08			192.168.168.1	192.168.168.10
210549	3	23.09.2021 8:49:51	23.09.2021 13:00:55			192.168.168.1	192.168.168.5
210550	106	23.09.2021 8:51:07	23.09.2021 10:02:38			192.168.168.1	192.168.168.12
210551	103	23.09.2021 8:52:02		3060	Unknown program... Startup denied	192.168.168.1	192.168.168.201
210552	19	23.09.2021 8:55:08	23.09.2021 16:53:51			192.168.168.1	192.168.168.8
210553	20	23.09.2021 9:07:00	23.09.2021 16:40:35			192.168.168.1	192.168.168.5
210554	13	23.09.2021 9:08:01	23.09.2021 16:15:24			192.168.168.1	192.168.168.10
210555	3	23.09.2021 9:09:21	23.09.2021 17:01:44			192.168.168.1	192.168.168.5
210556	76	23.09.2021 9:09:34	23.09.2021 16:28:07			192.168.168.1	192.168.168.14

Рис. 15. Фрагмент Log-файла подій в ІС пов'язаних з роботою засобів захисту інформації.

Таблиця 1.

Результати експериментів з контролю роботи засобів захисту інформації в ІС

№ події в ІС	**Розшифровка змісту події**
210547	а) старт АРМ №50 (IP 192.168.168.10) в 8:12:05 з підключенням до сервера БД з IP адресою 192.168.168.1. б) припинена робота АРМ №50 через перевищення встановленого часу (15хв.) його знаходження в неактивному стані в 8:40:01 – код помилки 1000.
210547	о 8:42:57 АРМ №50 повторно запущено і працювало в штатному режимі до 9:21:08.
210551	В 8:52:02 фоновий процес контролю ПЗ АРМ зафіксував заявку на запуск від АРМ №103 з IP адреси 192.168.168.201. При перевірці параметрів заявки виявилось, що АРМ 103 в дійсності зв'язаний з IP адресою 192.168.168.4, а не 192.168.168.201. В запуску було відмовлено, а сам факт спроби нелегального запуску (або невірно налаштованого ПЗ деякого АРМ) було зафіксовано в log-файлі подій в ІС з кодом помилки 3060.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Аналіз інтегрованих в апаратні та програмні компоненти ІС засобів захисту інформації ІС, які у своїй

сукупності утворюють комплексну підсистему захисту інформації, дозволив зробити висновки:

- сегментування мережі, виокремлення серверної частини в окрему під мережу з можливістю гнучкого налаштування політик безпеки для кожного сегмента підвищує стійкість ІС до атак ЗПЗ;

- застосування криптографічних засобів захисту гарантує відсутність несанкціонованого доступу до інформації в фізично неконтрольованих каналах передачі інформації, а також зменшує можливості ведення розвідки комп'ютерної мережі ІС;

- застосований метод запуску клієнтських АРМ з двохфакторною автентифікацією ПЗ та користувача унеможливлює підключення нелегальних програм та незареєстрованих копій штатного ПЗ;

- нетривіальні процедури контролю за операціями маніпулювання даними, виконання всіх операцій з даними під управлінням транзакцій гарантують цілісність та узгодженість інформації в ІС, а застосування контролю активності АРМ, гнучка дворівнева система управління наданням прав доступу до ресурсів ІС додатково зменшує вірогідність несанкціонованого доступу до інформації;

- автоматизована система резервного копіювання з територіальним розмежуванням місць зберігання копій та перевіркою їх робото здатності унеможливлює не відновлювану втрату інформації.

Проведені експерименти підтверджують працездатність засобів захисту інформації ІС та зроблені висновки. Реакція ІС на впливи, змодельовані в обох експериментах була очікуваною і в межах встановлених часових меж.

Таким чином, перелічені кроки методу забезпечення захисту інформації ІС в поєднані із організаційно-правовими заходами, використані як єдиний комплекс, дозволяють отримати технологію, застосування якої при розробці спеціалізованої ІС, гарантує високий рівень її захищеності її ресурсів від деструктивних впливів.

Література

1. Савенко О. С, Лисенко С. М. Дослідження методів антивірусного діагностування комп'ютерних мереж. Вісник Хмельницького національного університету. 2007. - №2(2). – С.120-125.

2. Lysenko S., Bobrovnikova K., Matiukh S., Hurman I., Savenko O. Detection of the botnets' low-rate DDoS attacks based on self-similarity. International Journal of Electrical and Computer Engineering, Vol. 10, Issue 4, 2020, Pages 3651-3659. DOI: http://doi.org/10.11591/ijece.v10i4.pp3651-3659.

3. Савенко ОС, Кльоц ЮП, Мостовий СВ. Дослідження та аналіз блокування процесів в комп'ютерній системі. Вісник ХНУ – 2007. - №3. – С.248-251.

4. Wawryn, K., Widuliński P. Detection of anomalies in compiled computer program files inspired by immune mechanisms using a template method. Journal of Computer Virology and Hacking Techniques. 2020. https://doi.org/10.1007/s11416-020-00364-w

5. Zeng J., Tang W. (2015) Negative Selection Algorithm Based Unknown Malware Detection Model. In: Gong M., Linqiang P., Tao S., Tang K., Zhang X. (eds) Bio-Inspired Computing - Theories and Applications. BIC-TA 2015. Communications in Computer and Information Science, vol. 562. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49014-3_53

6. Pomorova O. Metamorphic Viruses Detection Technique based on the the Modified Emulators [Text] / O. Pomorova, O. Savenko, S. Lysenko, A. Nicheporuk // CEUR-WS. – 2016. – Vol. 1614. – PP.375-383, ISSN: 1613-0073

7. Savenko, O., Nicheporuk, A., Hurman, I., Lysenko, S. - CEUR-WS. – 2019. – Vol. 2393. – P.633-643, ISSN: 1613-0073.

8. B. Savenko, S. Lysenko, K. Bobrovnikova, O. Savenko, G. Markowsky. Detection DNS Tunneling Botnets // Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS'2021, Cracow, Poland, September 22-25, 2021.

9. Xiang Yu, Hui Lu, Xianfei Yang, Ying Chen, Haifeng Song, Jianhua Li, Wei Shi An adaptive method based on contextual anomaly detection in Internet of Things through wireless sensor networks. International Journal of Distributed Sensor Networks 2020. Vol. 16(5) DOI: 10.1177/1550147720920478

10. Лукова-Чуйко Н. В. Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз: автореф. дис. ... д-ра техн. наук: 05.13.06, Київ, 2018, 40 с.

11. Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu. A survey of network anomaly detection techniques. Journal of Network and Computer Applications Vol. 60, January 2016. P. 19-31.

12. Bernadette J. Stolz, Jared Tanner, Heather A. Harrington, Vidit Nanda Geometric anomaly detection in data. Proceedings of the National Academy of Sciences Aug 2020, 117 (33) 19664-19669; DOI: 10.1073/pnas.2001741117

References

1. Savenko O. S, Lysenko S. M. Doslidzhennia metodiv antyvirusnoho diahnostuvannia kompiuternykh merezh. Herald of Khmelnitskyt National University. 2007. - №2(2). – S.120-125.

2. Lysenko S., Bobrovnikova K., Matiukh S., Hurman I., Savenko O. Detection of the botnets low-rate DDoS attacks based on self-similarity. International Journal of Electrical and Computer Engineering, Vol. 10, Issue 4, 2020, Pages 3651-3659. DOI: http://doi.org/10.11591/ijece.v10i4.pp3651-3659.

3. Savenko OS, Klots YuP, Mostovyi SV. Doslidzhennia ta analiz blokuvannia protsesiv v kompiuternii systemi. Visnyk KhNU – 2007. - №3. – S.248-251.

4. Wawryn, K., Widuliński P. Detection of anomalies in compiled computer program files inspired by immune mechanisms using a template method. Journal of Computer Virology and Hacking Techniques. 2020. https://doi.org/10.1007/s11416-020-00364-w

5. Zeng J., Tang W. (2015) Negative Selection Algorithm Based Unknown Malware Detection Model. In: Gong M., Linqiang P., Tao S., Tang K., Zhang X. (eds) Bio-Inspired Computing - Theories and Applications. BIC-TA 2015. Communications in Computer and Information Science, vol. 562. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49014-3_53

6. Pomorova O. Metamorphic Viruses Detection Technique based on the the Modified Emulators [Text] / O. Pomorova, O. Savenko, S. Lysenko, A. Nicheporuk // CEUR-WS. – 2016. – Vol. 1614. – PP.375-383, ISSN: 1613-0073

7. Savenko, O., Nicheporuk, A., Hurman, I., Lysenko, S. - CEUR-WS. – 2019. – Vol. 2393. – P.633-643, ISSN: 1613-0073.

8. B. Savenko, S. Lysenko, K. Bobrovnikova, O. Savenko, G. Markowsky. Detection DNS Tunneling Botnets // Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS2021, Cracow, Poland, September 22-25, 2021.

9. Xiang Yu, Hui Lu, Xianfei Yang, Ying Chen, Haifeng Song, Jianhua Li, Wei Shi An adaptive method based on contextual anomaly detection in Internet of Things through wireless sensor networks. International Journal of Distributed Sensor Networks 2020. Vol. 16(5) DOI: 10.1177/1550147720920478

10. Lukova-Chuiko N. V. Metodolohichni osnovy zabezpechennia funktsionalnoi stiikosti rozpodilenykh informatsiinykh system do kibernetychnykh zahroz: avtoref. dys. ... d-ra tekhn. nauk: 05.13.06, Kyiv, 2018, 40 s.

11. Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu. A survey of network anomaly detection techniques. Journal of Network and Computer Applications Vol. 60, January 2016. P. 19-31.

12. Bernadette J. Stolz, Jared Tanner, Heather A. Harrington, Vidit Nanda Geometric anomaly detection in data. Proceedings of the National Academy of Sciences Aug 2020, 117 (33) 19664-19669; DOI: 10.1073/pnas.2001741117