2. Sait Derzhavnoi sluzhby statystyky Ukrainy / [elektronnyi resurs] / Rezhym dostupu: http://www.ukrstat.gov.ua/
3. Zakon Ukrainy «Pro zakhody shchodo zakonodavchoho zabezpechennia reformuvannia pensiinoi systemy» / Rozdil pershyi / Stattia 1.

Статтю подано до редакції 11.02.2019 р.

УДК 65.012.8 DOI: 10.33111/mise.97.3

Бєгун А. В., к.е.н.,
професор кафедри інформаційного менеджменту,
Осипова О. І., к.е.н.,
доцент кафедри економіко-математичного моделювання,
Урденко О. Г.,
аспірант кафедри інформаційного менеджменту,
Київський національний економічний університет
імені Вадима Гетьмана

Biehun A. V., PhD in Economics,
Professor of the Information Management Department,
Osypova O. I., PhD in Economics,
Associate Professor of the Economic and Mathematical Modelling Department,
Urdenko O. G.,
Postgraduate Student of the Information Management Department,
Kyiv National Economic University named after Vadim Hetman

ПРО ОДИН З ІНСТРУМЕНТІВ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ABOUT ONE OF THE TOOLS OF THE ENTERPRISE INFORMATION SECURITY AUDIT

Анотація. *В умовах конвергенції економічних процесів та інформаційних технологій завжди існувала проблема збереження конфіденційності, дійсності та достовірності інформаційних ресурсів. Для розв'язання множини задач, які породжені визначеною проблемою, існують інструменти інформаційної безпеки (ІБ) функціонування економічних структур, що підтримують рівень цієї безпеки на відповідному надійному інтервалі. В статті представлено дослідження програмних засобів аудиту інформаційної безпеки (ІБ) підприємства. Для забезпечення додаткового рішення аудиту інформаційної безпеки підприємства авторами запропоновано скористатися власне розробленою програмною платформою — генератор формування звітів комп'ютерних експертиз. Функціонально платформа досліджує та фіксує дані наступних розділів: аудит з обстеження IT; технічний аудит IT; аудит IT бізнес-процесів; аудит визначення критеріїв IT; комплексний аудит IT; експертна оцінка стану IT; аудит інформаційної безпеки з визначенням ризиків виникнення інцидентів.*

Авторами класифіковано основні програмні інструменти аудиту інформаційної безпеки організаційної структури (підприємства), виконано аналіз їх переваг і недоліків, запропоновано програмну платформу «MAX CRIM WIN TOOLS», яка відповідно до міжнародних стандартів ІБ, враховує актуальні аспекти аналізу об'єкта ІТ за допомогою додаткового аудиту ІБ.
Доведено, що впровадження інструменту аудиту інформаційної безпеки організації
«MAX CRIM WIN TOOLS» допоможе розв'язати проблему, з якою постійно стикаються компанії: зменшення збитків від подій інцидентів інформаційної безпеки, факт яких в більшості випадків не є відомий, вибір і прийняття адекватних рішень стосовно мінімізації проблем забезпечення інформаційної безпеки, запобігання реалізації ризиків виникнення проактивних атак. Запропонований розроблений програмний комплекс «MAX CRIM WIN TOOLS» може бути інтегрований у вже існуючу СУІБ організації і може стати часткою нового проекту безпеки.
Ключові слова: *аудит, аудит інформаційної безпеки, модулі аналізу, програмна платформа, джерело загрози, інциденти інформаційної безпеки, експертна оцінка.*

Abstract*. In the context of convergence of economic processes and information technologies, there was always the problem of maintaining the confidentiality, validity and reliability of information resources. To address many of the problems posed by a particular problem, there are information security (IB) tools for the functioning of economic structures that maintain that security at an appropriate reliable interval. The article is devoted to the research of software tools of information security (IS) audit of the enterprise. To provide an additional information security audit solution, the authors propose to use a computer-generated reporting platform that has been developed. Functionally, the platform investigates and records the following sections: IT audit audit; IT technical audit; audit of IT business processes; audit of the definition of IT criteria; comprehensive IT audit; expert evaluation of the state of IT; information security audit to identify the risks of incidents.*
The authors classified the main software tools for information security audit of the organizational structure (enterprise), performed an analysis of their advantages and disadvantages, offered a software platform «MAX CRIM WIN TOOLS», which in accordance with international standards of IS, takes into account the current aspects of the analysis of the object of IT through additional audit IS.
It is proven that the implementation of the organization's information security audit tool «MAX CRIM WIN TOOLS» will help to solve a problem that is constantly faced by companies: reduction of losses from the events of information security incidents, the fact of which is in most cases not known, selection and making of adequate decisions to minimize the problems of providing information security, preventing the realization of risks occurrence of proactive attacks. The proposed developed software package «MAX CRIM WIN TOOLS» can be integrated into an existing ISMS of the organization and can become a part of a new security project.
Keywords: *audit, information security audit, analysis modules, software platform, threat source, information security incidents, peer review.*

Вступ. В умовах конвергенції економічних процесів та інформаційних технологій завжди існувала проблема збереження конфіденційності, дійсності та достовірності інформаційних ресурсів. Для розв'язання множини задач, які породжені визначе-

ною проблемою, існують інструменти інформаційної безпеки (ІБ) функціонування економічних структур, що підтримують рівень цієї безпеки на відповідному надійному інтервалі. Але, останнім часом, саме ІБ та її складові виявилися об'єктом дослідження суб'єктами інформаційних атак. Тому діючих кількісних та якісних важелів аналізу і контролю за самою системою ІБ та її керованістю вже недостатньо.

Для забезпечення комплексного рішення безпеки та моніторингу подій ІБ авторами [1, 2] запропоновано скористатися програмною платформою для моніторингу логів (журналів), яка базується на технології хмарних обчислень. Слід відмітити, що стосовно [2] у кожному домені на основі політики ІБ існують можливості здійснення моніторингу усіх процесів і визначення рівня інформаційної безпеки.

Однак, відповідно до терміну «платформа» виникає частина задач, які необхідно вирішувати в кожному домені ІБ [1]:

1) збір даних — логів від різних джерел інформації (журнали подій серверів і робочих станцій, мережеве активне обладнання, DLP-системи, IDS та IPS-системи, антивірусні програми);

2) нормалізація логів від різних джерел — процес переведення записів лог-журналів в єдиний стандартний вид;

3) фільтрація та кореляція подій безпеки;

4) стосовно політики безпеки домену, реєстрація деяких подій як інцидентів ІБ.

Світова практика забезпечення достатнього рівня інформаційної безпеки в різноманітних організаційних структурах представлена стандартами, політиками, методами, процедурами та функціями програмного забезпечення. Для отримання найбільш повної та об'єктивної оцінки стану захищеності підприємства, самої системи ІБ залучаються різноманітні засоби, які перевіряють спроможність реагувати на спроби проникнення і надання неправомірної шкоди організації. Одним із таких заходів є аудит системи менеджменту інформаційної безпеки.

Проблемам аудиту інформаційних технологій приділяли і приділяють закордонні та вітчизняні дослідники Тузик С.В., Сінглтон Т.В., Рудніцкий В.С., Петрик О.А. та інші. Але низька питань стосовно практичних інструментів аудиту систем інформаційної безпеки організаційних структур вивчена не на достатньому рівні. Для забезпечення додаткового рішення аудиту інформаційної безпеки авторами запропоновано скористатися власне розробленою програмною платформою — генератор формування звітів комп'ютерних експертиз [3].

Викладення основного матеріалу. При виконанні комплексу впроваджувальних робіт в організації, головною задачею постає аналіз бізнес-процесу з заданими критеріями якості та ефективності, які потребують визначення нестандартного оцінювання ризиків за допомоги пошуку уразливостей ресурсів та аналізу захищеності інформаційних систем. Тому залучення існуючих та розробка додаткових інструментів аудиту ІБ стають пріоритетними для ІТ-аудитора.

На сучасному ринку програмного інструментарію для аудиту ІБ представлено широкий спектр як універсальних, так і спеціалізованих апаратно-програмних засобів. Серед множини засобів слід виділити ті, які найчастіше застосовуються у практичній діяльності організаційних структур (табл. 1). Усі вони виконують загальновідомі задачі: аналіз поточних мір і політик ІБ, аналіз ІТ-структури компанії, аналіз існуючих ризиків.

Таблиця 1

АНАЛІЗ ПРОГРАМНИХ ІНСТРУМЕНТІВ АУДИТУ ІБ

	Назва програмного інструменту	Стислий опис властивостей	Результат/ Вартість
1.	Аналіз безпеки Microsoft	Інструмент можна використовувати для оцінки рівня прогалин в операційних системах Microsoft та важливих налаштувань, пов'язаних з безпекою.	Режим Інтернет-з'єднання/ Витрати: безкоштовно
2.	Тестер SSL Labs	Онлайн-сервіс інструмент виконує глибокий аналіз конфігурації будь-якого веб-сервера SSL у загальнодоступному доступі до Інтернету, допомагає оцінити якість зашифрованого зв'язку і написати детальний звіт.	Режим Інтернет-з'єднання/ Витрати: безкоштовно
3.	NMAP	Nmap (Мережевий сканер) підтримує різні типи сканування, такі як TCP, UDP, SYN, ICMP, FIN, FTP proxy, ACK — потужна програма для дослідження захисту комп'ютерних мереж, за допомоги якого виявляють хости, створюючи таким чином «карту» мережі.	Режим Інтернет-з'єднання/ Витрати: безкоштовно

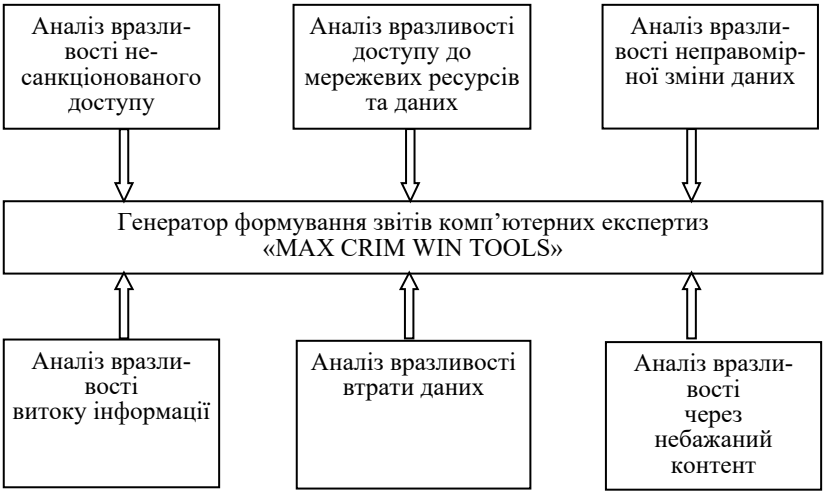
Закінчення табл. 1

	Назва програмного інструменту	Стислий опис властивостей	Результат/ Вартість
4.	OWASP ZAP	OWASP Zed Attack Proxy (ZAP) — простий у використанні інтегрований інструмент для тестування на проникання, який виявляє вразливі місця у веб-додатках.	Режим Інтернет-з'єднання/ Витрати: безкоштовно
5.	Splunk	Sptunk збирає, індексує і заносить (у режимі реального часу) дані реєстру у сховище пошуку, з якого може генерувати графіки, звіти, попередження, панелі приладів та візуалізація.	Режим Інтернет-з'єднання/ Витрати: безкоштовно для особистого використання (обмеження до 500 мегабайт на день)
6.	Fluxicon Disco	DISCO — інструмент процесу видобутку, який дозволяє аналізувати бізнес-процеси на основі реєстру подій. Головна ідея — видобувати знання з реєстру подій, записаного інформаційною системою.	Режим Інтернет-з'єднання/ Витрати: безкоштовно
7.	IDEA	IDEA — інструмент аналізу даних, призначений допомагати аудиторам швидко проводити аналіз даних, аби покращити аудити і виявити недоліки системи контролю. Важливими характеристиками є гарантія цілісності даних та забезпечення легкого аналізу понад 100 команд, пов'язаних з аудитом.	Режим Інтернет-з'єднання/ Витрати: на запит безкоштовно
8.	QlikView	QlikView — платформа бізнес-інтелекту, яку аудитори також можуть використовувати для аналізу даних. Можна використовувати системи Планування ресурсів підприємства як джерело даних.	Режим Інтернет-з'єднання/ Витрати: на запит завантаження безкоштовно
9.	BWISE	Рішення для програмного забезпечення з корпоративного управління, ризиків та дотримання законодавства, яке аудитори можуть використовувати для аудиту програмного забезпечення Планування ресурсів підприємства, таких як SAP і Oracle EBS.	Режим Інтернет-з'єднання/ Витрати: залежно від реалізації

**Джерело*: розроблено авторами

Стислий опис і властивості програмних засобів аудиту ІБ, які здійснюють свої функції або в он-лайн режимі, або прив'язані до мережевого з'єднання, неповністю охоплюють потреби організацій щодо обсягу даних для аналізу та їх якісних характеристик. Тому для вирішення поставлених вище завдань і моніторингу подій інформаційної безпеки, пропонується скористатися програмною платформою «MAX CRIM WIN TOOLS» [3], яка, відповідно до міжнародних стандартів ІБ, враховує актуальні аспекти об'єкта ІТ за допомогою додаткового аудиту ІБ. Продукт заснований на аналізі встановлених факторів і ознак статистичного зв'язку з іншими факторами або головними компонентами, що з певною ймовірністю ведуть до реалізації загроз або інших негативних наслідків, які необхідні експертам з інформаційної безпеки для підсумкової оцінки.

Технологія додаткового аудиту за допомогою програмної платформи [3], полягає в аналізі розподілених функцій, які класифікуються за видами властивостей порушень системи ІБ, і структурно представлена у вигляді модулів, що аналізують данні (рис. 1).



**Джерело*: розроблено авторами

Рис. 1. Структура програмної платформи «MAX CRIM WIN TOOLS»

Генератор формування звітів комп'ютерних експертиз «MAX CRIM WIN TOOLS» — це інструмент аналізу даних, призначений допомагати аудиторам оперативно отримувати систематизовану і достовірну інформацію для оцінки стану ІТ середовища компанії, аби виявляти недоліки системи і покращити аудит для прийняття рішень з управління ІТ.

Важливими характеристиками завдяки функціональному забезпеченню є надійність отримання цілісних систематизованих та об'єктивних даних, у вигляді зручних для перегляду звітів з поточного стану ІТ-середовища й оцінки ступеня їх відповідності обумовленим стандартам ІБ.

Програмна платформа — генератор формування звітів комп'ютерних експертиз «MAX CRIM WIN TOOLS» — це технологічний програмний інструмент, який базується на процесі видобутку з багаточисленних журналів операційної системи, системних програм і мережі, фактів загроз ІБ, які в подальшому фіксуються у комплексному звіті.

Функціонально платформа досліджує та фіксує дані наступних розділів: аудит з обстеження ІТ; технічний аудит ІТ; аудит ІТ бізнес-процесів; аудит визначення критеріїв ІТ; комплексний аудит ІТ; експертна оцінка стану ІТ; аудит інформаційної безпеки з визначенням ризиків виникнення інцидентів.

Дане програмне забезпечення допомагає експертам з інформаційної безпеки, аудиторам, системним аналітикам, командам технічної підтримки інформаційної безпеки, обробляти та аналізувати значні масиви даних журналів логів, які збираються із різноманітних джерел — програмних додатків, операційної системи та мережі та її налаштувань.

Програмне інструмент застосовується як комплекс, в якому користувач за допомогою функціональних команд (визначено словосполучення латинським алфавітом терміни, що визначають деякі поняття властивостей інформаційних технологій), запускає процес збирання даних у звіт до носія інформації. Таким носієм може бути накопичувач даних комп'ютера або інший носій, наприклад, USB-накопичувач.

Залежно від класифікації джерел загроз інформаційної безпеки, програмний засіб дає змогу збирати та аналізувати інформацію таких основних груп: небажаний контент, несанкціонований доступ, виток інформації, втрата даних, шахрайство, інформаційний тероризм (табл. 2).

Таблиця 2

КРИТИЧНІ ДАНІ, ЯКІ ОТРИМАНІ З МОЖЛИВИХ ДЖЕРЕЛ ЗАГРОЗ

	Група аналізу	Стислий опис	Результат
1.	Вразливості та важелі несанкціонованого доступу	Мережевий моніторинг процесів для виявлення несанкціонованих з'єднань: FTP; Filezilla; vpn; OpenSSH; Putty; RDP; ключі бездротової мережі (WEP / WPA)	Детальний звіт
2	Вразливості доступу до мережевих ресурсів та даних	Сканування комп'ютерів та ідентифікація застосованих користувачем у тому числі несанкціонованих паролів у: сховищах LSA; LM/NT; корпоративної мережі; RAS/VPN; Dialup/VPN; бездротової мережі (WEP/WPA); записи DNS (MX, NS, A, SOA)	Детальний звіт
3.	Вразливості неправомірної зміни даних	Сканування локальної історії подій реєстру ОС Windows — програма знаходить зашифровані дані в Реєстрі, відображає розшифровані дані	Детальний звіт
4.	Вразливості витоку інформації	Сканування комп'ютерів та ідентифікація застосованих користувачем у тому числі несанкціонованих даних: дампах пам'яті ОС і програм; аналіз планувальника завдань ОС; облікових записах відомих Інтернет миттєвих повідомлень — месенджерів	Детальний звіт
5.	Вразливості втрати даних	Сканування комп'ютерів та ідентифікація несанкціонованої модифікації, видалення даних у ОС — відновлення даних	Детальний звіт
6.	Вразливості через небажаний контент	Сканування інтернет-трафіку. Сканування журналів і кеш веббраузерів: Firefox, Chrome, Opera, Internet Explorer, Microsoft Edge.	Детальний звіт

**Джерело*: розроблено авторами

До найбпоширеніших джерел, з яких здійснюється вибірка даних лог-файлів, index-файлів, файлів реєстру ОС, баз даних для аналізу необхідно віднести:

1) операційна система — Windows;

2) програмні додатки та сервіси, бази даних, реєстри:

2.1) журнали Інтернет-історії (посилання та її довжина, час візиту на сайт, назва відвіданого ресурсу, браузер і його версія) та кеш веб-браузерів: Internet Explorer (версія 4.0 — 11.0), Microsoft Edge, Mozilla Firefox (Усі версії), Google Chrome та Opera:

2.2) журнали та кеш веб-браузерів, які зв'язані з соціальними мережами та електронною поштою: Facebook, Yahoo, Google та GMail;

2.3) бази даних, журнали та кеш поштових клієнтів: Microsoft Outlook 2002 — 2018, Windows Mail, IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird;

2.4) Журнали програм мережевого з'єднання: Microsoft Remote Desktop Connection всередині файлів .rdp.;

2.5) Реєстр операційної системи шифровані ключі — LSA, LM/NT;

2.6) Журнали програм мережевого моніторингу, які відображають усі відкриті на даний момент порти TCP / IP та UDP;.

2.7) журнали програм бездротового мережевого моніторингу, які відображають інформацію різних джерел запущених в операційній системі та відображають таку інформацію: IP-адреса, MAC-адреса, компанія, яка виготовила мережеву карту, й, можливо, назва комп'ютера;

2.8) журнали операційної системи, що фіксують мережеві ресурси з усіх доменів/робочих груп, включаючи приховані спільні ресурси та ресурси, які зареєстровані за адміністраторами;)

2.9) журнали програм з даними про запущені в операційній системі DNS (MX, NS, A, SOA);

2.10) журнали операційної системи, в яких міститься інформація про події, які відбуваються та колись відбулися на цьому комп'ютері;

2.11) журнали операційної системи в яких міститься інформація про USB-пристрої, які в даний час підключені до комп'ютера, а також усі USB-пристрої, що були застосовані раніше;

2.12) Журнали, які збирають інформацію програми Skype та відображають дані про вхідні/вихідні дзвінки, повідомлення чату та передачу файлів, що здійснені вказаним обліковим записом Skype;

2.13) системні журнали, які фіксують усі приховані альтернативні потоки і вказують на паралельні процеси у системі;

2.14) системні журнали, які фіксують усі створені файли та папки.

Системні журнали, які фіксують зміни списку статичних пунктів меню, що з'явились у контекстному меню при натисканні правою кнопкою миші на файл / папку в Провіднику Windows;

2.16) дамп-системи й журнали планувальника завдань;

2.17) журнали та реєстр інстальованого ПЗ і розширений його аналіз;

2.18) журнали з інформацією про локальну історію дій користувачів за весь час існування Windows на ПК за датою створення (відкриття папок / файлів; вихід у мережу; тривалість роботи/виключення/сну ПК; інстальовані та видалені програми);

2.19) Журнали та реєстр Product ID/KEY: ключів ОС Windows; Microsoft Office; Visual Studio; SQL Server;

2.20) Логіни та паролі, облікових записів з останніх версій браузерів: Opera; Firefox; Microsoft Edge / Internet Explorer; Chrome (в тому числі, збір паролів з браузера Firefox за захистом майстер-паролем).

У процесі проведення дослідження у реальному форматі часу за обраними користувачем критеріями аналізу у головному меню програмної платформи «генератор формування звітів комп'ютерних експертиз «MAX CRIM WIN TOOLS», проводиться автоматично аналіз та збирання інформації про визначені події стану ІБ системи, які фіксуються у розділах звіту. Інтерфейс користувача програмної платформи представлений у вигляди робочих вікон, форму яких наведено на рис. 1.

Рис. 1.а) «Дослідницькі інструменти»

Рис. 1.б) «Відновлення паролів»

Рис. 1. в) «Мережеві інструменти»

Рис. 1. г) «Збереження звіту»

Результати проведеного дослідження представлено у вигляді «Аудит безпеки» (рис. 2).

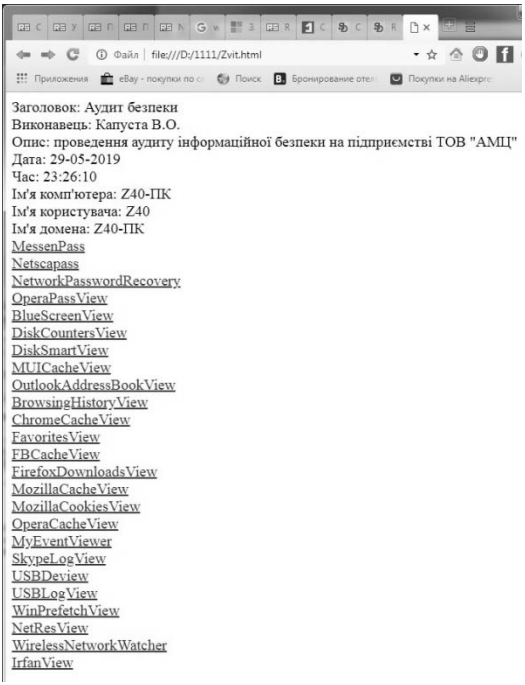
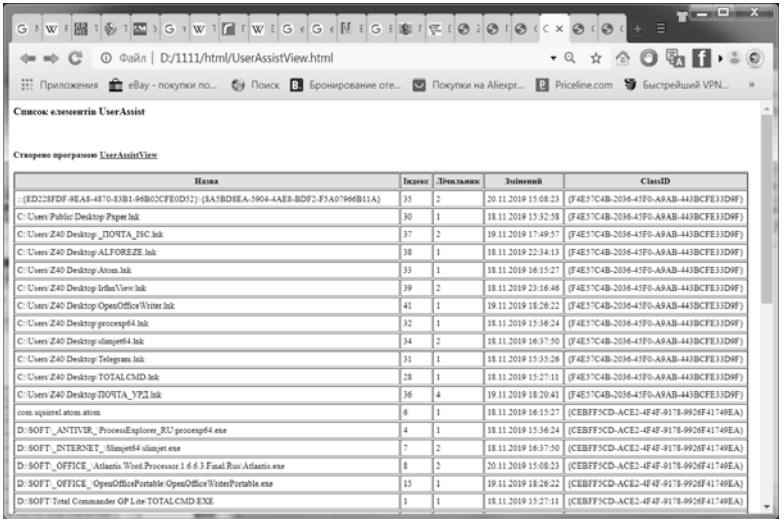


Рис. 2. Розділи формування загального звіту

Деталізація кожного розділу має загальні особливості та представлена одним із фрагментів (рис. 3). Усі записи містять інформацію про файли формату .exe та посилання, які користувач системи часто використовує. Дані зберігаються в реєстрі операційної системи за ключем HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist.



Назва	Індекс	Лічильник	Змінений	ClassID
{1ED228FDF-9EA8-4870-83B1-96B02CFE0D52} ({A5BD8EA-5904-4AE8-BDF2-F5A07966B11A)	35	2	20.11.2019 15:08:23	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users Public Desktop Paper.lnk	30	1	18.11.2019 15:32:58	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop_ПОШТА_ISC.lnk	37	2	19.11.2019 17:49:57	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\ALFOREZE.lnk	38	1	18.11.2019 22:34:13	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\Atom.lnk	33	1	18.11.2019 16:15:27	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\IrfanView.lnk	39	2	18.11.2019 23:16:46	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\OpenOffice\Writer.lnk	41	1	19.11.2019 18:26:22	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\procexp64.lnk	32	1	18.11.2019 15:36:24	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\slimjet64.lnk	34	2	18.11.2019 16:37:50	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\Telegram.lnk	31	1	18.11.2019 15:35:26	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\TOTALCMD.lnk	28	1	18.11.2019 15:27:11	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
C:\Users\Z40\Desktop\ПОШТА_УРД.lnk	36	4	19.11.2019 18:20:41	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
com.squirrel.atom.atom	6	1	18.11.2019 16:15:27	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
D:\SOFT_ANTIVIR_ProcessExplorer_RU\procexp64.exe	4	1	18.11.2019 15:36:24	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
D:\SOFT_INTERNET_Slimjet64\slimjet.exe	7	2	18.11.2019 16:37:50	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
D:\SOFT_OFFICE_Atlantis Word Processor 1.6.6.3 Final Rus\Atlantis.exe	8	2	20.11.2019 15:08:23	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
D:\SOFT_OFFICE_OpenOfficePortable\OpenOfficeWriterPortable.exe	15	1	19.11.2019 18:26:22	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
D:\SOFT\Total Commander GP Lite\TOTALCMD.EXE	1	1	18.11.2019 15:27:11	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}

Рис. 3. Звіт відображає список записів UserAssist

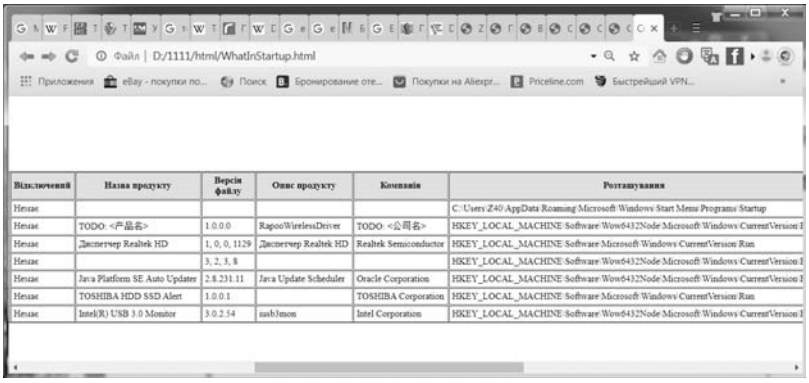
Усі програми автоматично завантажуються при запуску Windows. Для кожної програми відображається така інформація: тип запуску (папка реєстру/запуску), зміст командного рядка, назва продукту, версія файлу, назва компанії, розташування в реєстрі або у файловій системі тощо (рис. 4).

Порівняльний аналіз отриманих таблиць дозволяє визначити основні переваги використання розробленого генератора формування звітів комп'ютерних експертиз для збору та аналізу різноманітних даних:

- збір логів без використання спеціальних агентів, які необхідно додатково встановлювати та оновлювати;
- автоматизований «парсинг» — розбір подій, тобто можливість автоматичного вилучення окремих даних;
- потужні можливості збору: повний збір вказаних даних, збір даних за окремо вибраними функціями, логічними змінними. Також забезпечується фільтрація даних лог-форматів;

- необмежена кількість збережених пошуків — будь-який контекстний пошук може бути збережений для подальшого використання;
- функції інтерфейсу забезпечують інтуїтивно зрозумілий алгоритм виконання запитів обираючи параметри з меню;
- можливість додати необмежену кількість користувачів до створює мого звіту;
- можливість надсилати необмежений об'єм лог-даних під час використання програмного комплексу.

Рис. 4. Звіт з відображанням списку програм



Продовження рис. 4

Висновки. Розробка і впровадження інструментів аудиту інформаційної безпеки організації у відповідності з кращими практиками створює умови для переконання дійсності та ефек-

тивності самого процесу. Цей процес украй необхідний тоді, коли організація оперує великими обсягами конфіденційної інформації, наприклад, інформацією про своїх клієнтів.

Запропонований розроблений програмний комплекс «MAX CRIM WIN TOOLS» може бути інтегрований у вже існуючу СУІБ організації і може стати часткою нового проекту безпеки. Його впровадження забезпечить:

- надання процесам необхідної інформації для проведення аналізу та виявлення ризиків інформаційної безпеки;
- попередження інцидентів у системі інформаційної безпеки в майбутньому, ефективно реагувати на динаміку їх виникнення;
- надання процесам оперативної інформації для моніторингу ефективності швидких рішень.

Таким чином, можна зробити висновок, що впровадження інструменту аудиту інформаційної безпеки організації «MAX CRIM WIN TOOLS» допоможе розв'язати проблему, з якою постійно стикаються компанії: зменшення збитків від подій інцидентів інформаційної безпеки, факт яких у більшості випадків не є відомий, вибір і прийняття адекватних рішень стосовно мінімізації проблем забезпечення інформаційної безпеки, запобігання реалізації ризиків виникнення проактивних атак.

Література

1. Бєгун А. В. Особливості перевірки властивостей безпеки програм методом статичного аналізу // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. №88. — К. : КНЕУ, 2013. — С.132–138.

2. Бєгун А. В., Осипова О. І., Урденко О. Г. Ситуаційний логменеджмент інформаційної безпеки підприємства // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. №95. — К. : КНЕУ, 2018. — С. 18–29.

3. Бєгун А. В., Урденко О. Г. Програмне забезпечення «Генератор формування звітів комп'ютерних експертиз MAX CRIM WIN TOOLS» Авторське свідоцтво №82338 від 19.10.2018 р.

4. Biehun A., Ignatova Iu. Estimation the reliability of the elements of cloud services. // Operations Research and Decisions. — Wroclaw: Wroclaw University of Technology, 2017. — Vol. 27(3), — Pg. 65–80.

References

1. Biehun A. V. Analiz zagroz informaciyi portalu cherez ataky na dodatky [Analysis of portal information threats by attack on applications]//

Modelyuvannya ta informacijni systemy v ekonomici. Mizhvidomchyj nauk. zbirnyk. Vol.№ 80. — K:. KNEU, 2009. — S. 101–107: [in Ukrainian].

2. Galicyn V. K. Systemy monitoryngu: Monografiya [Monitoring systems: Monograph]. — K.: KNEU, 2000. — 231 s: [in Ukrainian].

3. Kaminskyj O. Ye. Xmarni texnologiyi v paradygmi informacijnoyi ekonomiky: monografiya [Cloud technologies in the information economy paradigm: monograph] / O. Ye. Kaminskyj. — K.: KNEU, 2018. — 230 s: [in Ukrainian].

4.Biehun A., Ignatova Iu. Ocinka nadijnosti elementiv hmarnyh servisiv [Estimation the reliability of the elements of cloud services] //Operations Research and Decisions. — Wroclaw: Wroclaw University of Technology, 2017. — Vol. 27(3), — Pg. 65–80: [in English].

Статтю подано до редакції 12.02.2019 р.

УДК 004.9:004.738.52 DOI: 10.33111/mise.97.4

Василів В. Б., к.т.н.,
доцент кафедри комп'ютерних технологій
та економічної кібернетики,
Національний університет водного господарства
та природокористування
Василів Б. В., магістр спеціалізації
«Інформаційні управляючі системи та технології»**,**
Київський національний економічний університет
ім. Вадима Гетьмана

Vasyliv V. B., PhD in Engineering,
Associate Professsor of the Computer Technology and Economic Cybernetics Department, National University of Water and Environmental Engineering
Vasyliv B.V., Master Student
at the «Information management systems and technology» pseciality
Kyiv national economic university
named after Vadim Hetman»

КЛІЄНТООРІЄНТОВАНИЙ АГРЕГАТОР МАСОВИХ ВІДКРИТИХ ОНЛАЙН КУРСІВ

CLIENT-ORIENTED AGGREGATOR OF MASSIVE OPEN ONLINE COURSES

Анотація. *Поряд з традиційними моделями освіти все більшого розповсюдження знаходять технології дистанційної освіти. Встановлено, що технології дистанційної освіти і використання цифрового освітнього контенту сприяють розширенню доступу до освіти. Ринок онлайн-освіти зростає і розвивається як в Україні, так і за кордоном. Для полегшення пошуку серед онлайн курсів існують спеціалізовані сайти-*