DOI: 10.18372/2410-7840.20.12453
УДК 351.746:007-047.44

АНАЛІЗ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Володимир Гур'єв, Ярослав Усов

На сьогоднішній день бездротові корпоративні інформаційні системи є невід'ємною складовою конкурентного функціонування сучасного підприємства. Зручність використання, майже не обмежений функціонал, не висока вартість розгортки систем – це основні переваги даного типу систем. Оскільки конфіденційна інформація підприємства (електронні пошти, паролі до облікових записів, реквізити доступу до серверів, хеш-дані облікових записів користувачів та інша інформація, якої немає у відкритому доступі) є метою для багатьох кіберзлочинців, дані технології часто підлягають атакам різного роду. Таким чином, проблема визначення та аналізу вразливості інформаційної безпеки в корпоративних інформаційних системах є актуальною на сьогоднішній день. Проводячи аналіз ми спирались на дослідження зарубіжних вчених та практикуючих компаній, що займаються вивченням загроз та розробкою систем їх запобігання. Дослідження даного питання дає можливість визначити та класифікувати можливі загрози та модернізувати існуючі або розробити нові ефективні методи та заходи інформаційної безпеки.

Ключові слова: *корпоративні інформаційні системи, комп'ютерні мережі, загрози інформаційної безпеки, захист інформації.*

Постановка проблеми. Корпоративні інформаційні системи міцно увійшли в наше життя. У сучасному світі досить складно уявити собі підприємство, яке успішно розвивається і керується без участі такої системи. У зв'язку з тим, що в корпоративних інформаційних системах зберігається інформація, порушення цілісності або конфіденційності якої може привести до краху цілого підприємства гостро стоїть питання про захист інформації в корпоративних інформаційних системах. Причому мова йде не тільки про запобігання витоку корпоративної інформації, зниження обсягів паразитного трафіку і відбитті атак на ресурси компанії, але і про оптимізацію роботи системи в цілому. Знайти універсальне рішення в даному питанні практично неможливо: неоднорідність сфер діяльності і структур організацій переводить завдання в категорію яка потребує індивідуального підходу. Захист систем даного типу має спиратися на аналізі основних можливих вразливостей.

Аналіз останніх досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В.В. Баранника, В.М. Богуна, В.М. Базилевича, С.В. Віхорева, І.Д. Горбенко, Ю.І. Грицюк, С.В. Казмирчук, Г.Ф. Конаховича, О.Г. Корченка, В.А. Лахно, М.Г. Луцького, А.І. Марущака, В.В.Мохора, В.П. Мельнікова, О.М. Новікова, О.В. Олійника, О.В. Сосніна, С.В. Толюпи, В.О. Хорошко, О.К. Юдіна та ін.

Дослідження різноманітних аспектів інформаційно-аналітичної діяльності здійснювали Т.В. Абрамова, С.С. Алдишев, В.П. Александрова, А.А. Атаян, С.Ф. Багаундінова, Т.В. Вдовіна, А.В. Горячов, Р.О. Гуревич, М.І. Жалдак, О.П. Значенко, В.Г. Кальченко, Н.В. Кисіль, В.І. Клочко, Н.В. Морзе, С.Ю. Нікіфорова, О.В. Пархоменко, С.А. Раков, М.В. Селіна, Ю.М. Ткач, В.А. Сластьонін та ін.

Виділення не вирішених раніше частин загальної проблеми. На сьогоднішній день недостатньо дослідженою залишилась проблема визначення основних типів загроз інформаційної безпеки корпоративних інформаційних систем.

Мета статті. Головною метою цієї роботи є аналіз основних типів загроз інформаційної безпеки в корпоративних інформаційних системах.

Виклад основного матеріалу.

Корпоративна інформаційна система (КІС) – це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві (в корпорації) і постачає інформацію для прийняття управлінських рішень. У ній реалізована управлінська ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології [1]. В загальному випадку КІС – це система з можливістю масштабування, призначена для комплексної автоматизації всіх видів господарської діяльності великих і середніх підприємств, в тому числі корпорацій, що складаються з групи компаній, які потребують єдиного управління. Об'єднує систему управління персоналом, матеріальними, фінансовими та іншими ресурсами компанії, використовується для підтримки планування і управління компанією, для підтримки прийняття управлінських рішень її керівниками. Під КІС можна розуміти управлінську ідеологію, яка об'єднує бізнес-стратегію та інформаційні технології.

До основних принципів побудови КІС належать:

– інтелектуальність (управління організацією – реєстрація та накопичення інформації);

– інтегрованість (наскрізне проходження документів через різні служби);

– модульність (можливість поетапного впровадження системи);

– доступність;

– відкритість (можливість взаємодіяти з іншими програмами);

– адаптивність (потужність механізму налаштувань).

Основні вимоги КІС:

– використання архітектури клієнт-сервер з можливістю застосування промислових СУБД;

– забезпечення безпеки методами контролю і розмежування доступу до інформаційних ресурсів;

– підтримку розподіленої обробки інформації;

– модульний принцип побудови з оперативно-незалежних функціональних блоків з розширенням за рахунок відкритих стандартів (API, COM і інші).

Корпоративні інформаційні системи діляться на наступні класи:

– ERP (Enterprise Resource Planning System);

– CRM (Customer Relationship Management System);

– MES (Manufacturing Execution System);

– WMS (Warehouse Management System);

– EAM (Enterprise Asset Management);

– HRM (Human Resource Management);

– СЕД (Системи електронного документообігу).

Підходи побудови КІС:

– орієнтація на споживача;

– процесний підхід;

– збалансована система показників (відношення клієнта до компанії, ступінь його задоволеності, інноваційний потенціал компанії і співробітників, якість бізнес-процесів та ін.);

– комплексний підхід до управління;

– системний підхід;

– адаптивне управління (вибір оптимального способу досягнення мети, це спосіб управління, при якому зберігаються незмінними цільові показники).

Головними особливостями сучасного підходу до побудови корпоративної інформаційної системи підприємства є:

– всебічний аналіз бізнес-процесів, на основі якого проводиться розробка проекту інформаційної системи і обґрунтування закладених в ньому рішень;

– використання широкої палітри сучасних методологій та інструментальних засобів моделювання та проектування систем;

– підтримка міжкорпоративного бізнесу;

– детальне опрацювання та узгодження з замовником всіх етапів розробки проекту, контрольних точок, необхідних ресурсів.

Такий підхід забезпечує розробку інтегрованих рішень, побудованих на об'єктивних даних про роботу підприємства, своєчасне узгодження всіх принципових питань між замовником, генеральним підрядником та іншими учасниками робіт і направлений на збереження зроблених в систему інвестицій.

Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи. Для більшості корпорацій з розподіленою інфраструктурою процес безперервного забезпечення комплексного захисту інформаційних активів стає непростим завданням через високу складність архітектури і велику кількості взаємозв'язків всередині окремих підсистем [2]. За результатами аналітики [8] в 2017 році найбільш поширені уразливості на мережевому периметрі корпоративних інформаційних систем розподілені наступним чином (див. рис. 1).

Локальна обчислювальна мережа є основою функціонування будь-якої КІС. До найбільш поширених загроз інформаційної безпеки даного типу мереж належать:

1. Недоліки захисту службових протоколів, що призводять до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі.

2. Словникові паролі.

3. Недостатній рівень захисту привілейованих облікових записів.

4. Зберігання важливої інформації у відкритому вигляді.

5. Недоліки захисту протоколів NBNS і LLMNR.

6. Недостатньо ефективна реалізація антивірусного захисту.

7. Використання слабких алгоритмів шифрування при зберіганні паролів.

8. Уразливі версії програмного забезпечення.

9. Надлишкові привілеї додатків або СУБД.

10. Використання відкритих (незахищених) протоколів передачі даних.

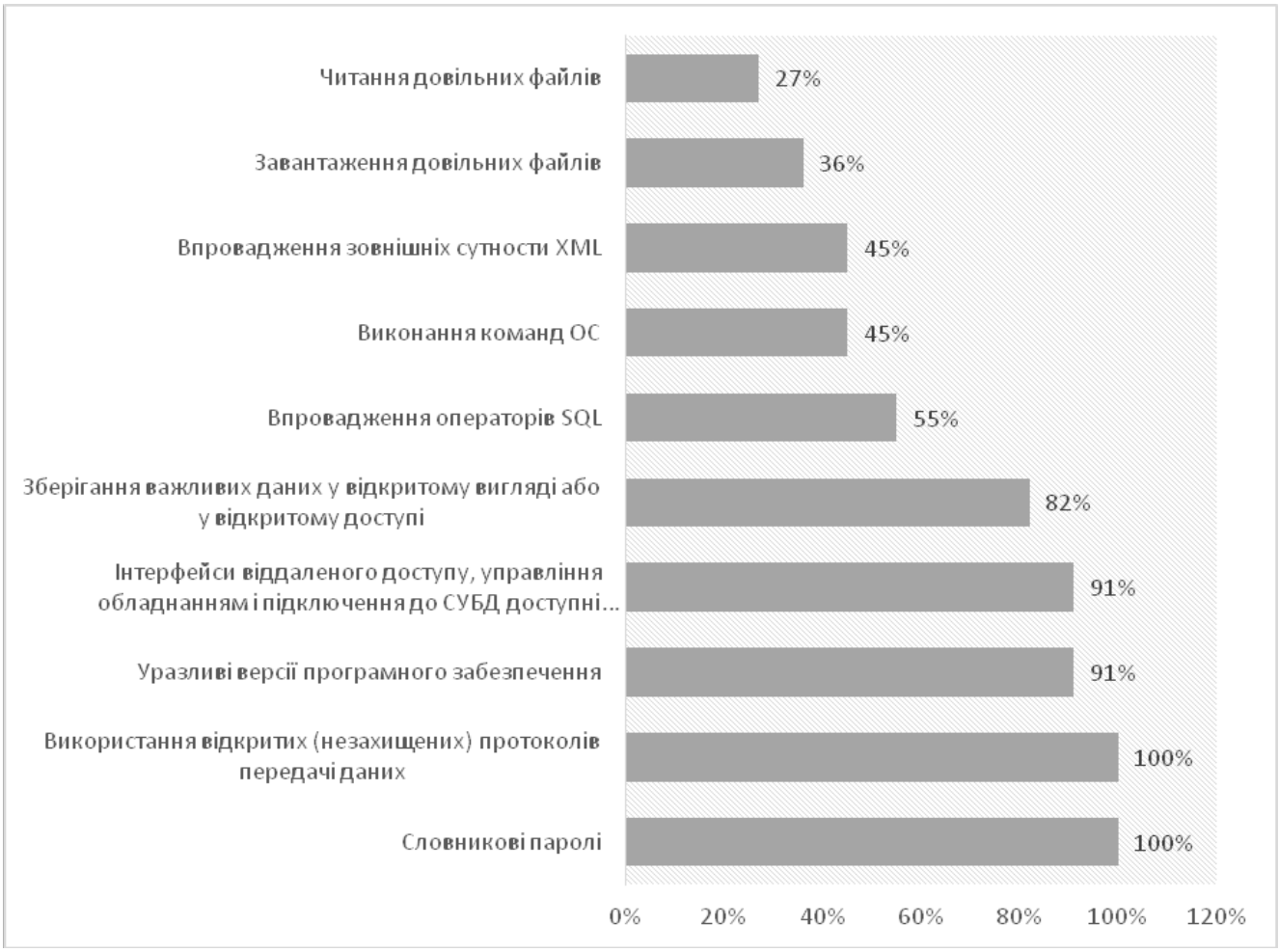

Рис. 1. Найбільш поширені уразливості на мережевому периметрі (частка систем)*
**Джерело за даними аналітики компанії Positive Technologies 2017 рік [8].*

З точки зору безпеки, слід враховувати не тільки загрози, властиві провідним мережам, але також і середу передачі сигналу. У бездротових мережах отримати доступ до переданої інформації набагато простіше, ніж в провідних мережах, так само як і вплинути на канал передачі даних. Досить помістити відповідний пристрій в зоні дії мережі [2]. До основних загроз інформаційної безпеки в мережах стандарту 802.11 нами було віднесено чужинців, тобто пристрої що надають можливість неавторизованого доступу до корпоративної мережі, нефіксовану природу зв'язку та вразливості мережевих пристроїв. Оскільки ефір є середовищем із загальним доступом, кожен невірно конфігурований клієнт, або збій антени точки доступу можуть створювати проблеми, як на фізичному, так і на канальному рівні, приводячи до погіршення якості обслуговування інших клієнтів мережі.

В той же час корпоративні інформаційні системи мають свої характерні вразливості інформаційної безпеки. До них можна віднести:

1. Помилки в коді веб-додатків і відсутність оновлень безпеки.

2. Недоліки конфігурування.

За даними результатів аналітики провідних компаній, які займаються інформаційною безпекою підприємств [8] останніми роками зберігається тенденція до підвищення загального рівня захищеності мережевого периметра корпоративних інформаційних систем. В середньому, у 27% випадків фахівцям не вдається подолати мережевий периметр і отримати доступ до ресурсів внутрішньої локальної обчислювальної мережі [6]. Дані результати пов'язані з тим, що деякі замовники регулярно проводять тестування на проникнення і усувають виявлені вразливості. Однак важливо пам'ятати, що конфігурація мережевої інфраструктури регулярно змінюється, тому тестування на проникнення необхідно проводити на регулярній основі. Крім того, потрібно стежити за тим, які служби доступні для підключення з мережі Інтернет. Приклади подолання периметра і отримання доступу до ресурсів локальної обчислювальної мережі:

1. Тривіальна складність подолання периметра. На периметрі мережі доступний для підключення інтерфейс налагодження JDWP. Будь-який

зовнішній порушник може використовувати загальнодоступний експлойт (github.com/IOActive / jdwp-shellifier) і виконати довільні команди на сервері. Використовуючи цю вразливість і надлишкові привілеї служби, вдається отримати повний контроль над сервером і доступ до ЛВС (якщо на вузлі є доступ до інтерфейсу внутрішньої мережі).

2. Низька складність подолання периметра. На тестованому вузлі виявлено веб-додаток для управління навчанням співробітників. Шляхом реєстрації нового облікового запису без підтвердження особи вдається отримати доступ до функціональності веб-додатка і завантажити веб-інтерпретатор командного рядка (веб-шелл) на сервер, що робить можливим виконання довільних команд ОС на сервері з привілеями веб-додатка. Таким чином вдається отримати доступ до ЛОМ, у випадку, коли на вузлі є доступний інтерфейс внутрішньої мережі.

3. Середня складність подолання периметра. В ході робіт по оцінці обізнаності співробітників в питаннях інформаційної безпеки була проведена масова розсилка електронних листів від внутрішньої особи з посиланням на веб-ресурс, що містить фішингову форму для введення облікових даних. Деякі співробітники ввели облікові дані в помилкову форму аутентифікації. Отримані облікові дані можуть бути використані для несанкціонованого доступу до ресурсів системи. Для використання фішингових сценаріїв атак як мінімум необхідно зареєструвати власний домен і розробити неправдиву форму аутентифікації. Більш того, важливо зробити фішинговий ресурс максимально наближеним по дизайну сторінки до того ресурсу, яким звик користуватися співробітник. Для цього необхідно проводити додаткові розвідувальні дії, що істотно підвищує складність реалізації атаки.

Після отримання доступу до внутрішньої мережі зовнішній зловмисник має можливості для розвитку атаки і отримання повного контролю над всією IT-інфраструктурою або окремими критично важливими системами [6].

У більшості випадків для отримання максимальних привілеїв у критично важливих системах від імені внутрішнього порушника досить підібрати обліковий запис з привілеями локального адміністратора на одній з робочих станцій або на сервері ЛОМ, запустити спеціалізоване ПО і отримати у відкритому вигляді облікові записи локальних адміністраторів інших вузлів. Даний вектор атаки можна розвивати аж до отримання облікових даних адміністраторів доменів.

За результатами звітів компаній [8], діяльністю яких є аналіз та захист інформаційної безпеки підприємств, перше місце в рейтингу найбільш поширених вразливостей захисту внутрішніх ресурсів належить недолікам захисту протоколів мережевого і канального рівнів, що призводить до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі. Кожна досліджувана система містила різні недоліки захисту службових протоколів, таких як ARP, STP, BOOTP, CDP. У кожному з проектів, де проводився аналіз мережевого трафіку ЛОМ, було виявлено відсутність механізмів захисту від атак ARP Cache Poisoning. Даний недолік може бути використаний для прослуховування трафіку в мережі і проведення атак типу «людина посередині» [2]. В ході успішної реалізації атаки порушник може перехоплювати конфіденційну інформацію, змінювати дані в процесі передачі і блокувати мережеву взаємодію.

На другому місці серед вразливостей внутрішніх мереж знаходиться використання словникових паролів. Третє місце – недостатній рівень захисту привілейованих облікових записів.

Таким чином, можна зробити наступні висновки: сучасні корпоративні інформаційні системи мають велику кількість вразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації. Досить низьким є рівень захищеності бездротових мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки.

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених вразливостей і недоліків, для усунення яких, як правило, досить застосувати базові принципи забезпечення інформаційної безпеки:

1) використовувати сувору парольний політику;
2) захищати привілейовані облікові записи;
3) не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі;
4) обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб;
5) захищати або відключати в локальної обчислювальної мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;
6) мінімізувати привілеї користувачів і служб;
7) регулярно оновлювати ПО і встановлювати оновлення безпеки ОС;
8) для своєчасного виявлення атак використовувати SIEM-системи;
9) для захисту веб-додатків використовувати web application firewalls;

10) проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки (при цьому важливо проводити і оцінку ефективності таких тренінгів);

11) для захисту від поширення шкідливого ПЗ із застосуванням соціальної інженерії використовувати спеціалізовані антивірусні рішення;

12) регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці.

При цьому важливо забезпечити всі ці заходи в комплексі, тільки тоді захист буде ефективним, а витрати на різні дорогі рішення виявляться виправданими.

ЛІТЕРАТУРА

[1]. Е. Фролов, "Современные концепции управления в производственной логистике, MES для дискретного производства — метод вычисляемых приоритетов", *САПР и графика*, № 1, С. 71-75, 2011.

[2]. В. Базилевич, "Аналіз методів захисту від кіберзагроз в бездротових мережах стандарту IEEE 802.11", *Захист інформації*, №3, С. 222-227, 2017.

[3]. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/1126-97-%D0%BF

[4]. А. Корченко, Е. Иванченко, С. Казмирчук, "Анализ и определение понятия риска для его интерпретации в области информационной безопасности", *Защита информации*, №3, 2010.

[5]. О. Корченко, *Системи захисту інформації* , *монографія,* К.: НАУ, 2004, 264 с.

[6]. Практическая атака на беспроводную сеть с WEP шифрованием [Електронний ресурс]. Режим доступу: http://habrahabr.ru/post/92681/

[7]. IBM 2015 Cyber Security Intelligence Index [Електронний ресурс]. Режим доступу: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

[8]. Актуальные киберугрозы: III квартал 2017 года [Електронний ресурс]. Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/

АНАЛИЗ УЯЗВИМОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

На сегодняшний день беспроводные корпоративные информационные системы являются неотъемлемой составляющей конкурентного функционирования современного предприятия. Удобство использования, почти не ограниченный функционал, не высокая стоимость развертки систем - это основные преимущества данного типа систем. Поскольку конфиденциальная информация предприятия (электронные почты, пароли к учетным записям, реквизиты доступа к серверам, хэш-данные учетных записей пользователей и другая информация, которой нет в открытом доступе) является целью для многих киберпреступников, данные технологии часто подлежат атакам разного рода. Таким образом, проблема определения и анализа уязвимостей информационной безопасности в корпоративных информационных системах является актуальной на сегодняшний день. Проводя анализ мы опирались на исследования зарубежных ученых и практикующих компаний, занимающихся изучением угроз и разработкой систем их предотвращения. Исследование данного вопроса дает возможность определить и классифицировать возможные угрозы и модернизировать существующие или разработать новые методы и меры информационной безопасности.

Ключевые слова: корпоративные информационные системы, компьютерные сети, угрозы информационной безопасности, защита информации.

ANALYSIS OF CORPORATE INFORMATION SYSTEMS VULNERABILITY

For today, wireless corporate information systems are an integral part of the competitive functioning of a modern enterprise. Ease of use, almost unlimited functionality, not high cost system scan - these are the main advantages of this type of systems. Corporate information systems of large companies regularly undergo changes - the hardware configuration is updated, the network topology changes, new nodes and system targets are emerging. For most corporations with distributed infrastructure, the process of continuous provision of comprehensive protection of information assets becomes a daunting task due to the high complexity of architecture and a large number of interconnections within individual subsystems. According to the results of analytical studies of leading companies that deal with information security of enterprises in recent years, the tendency to increase the overall level of security of the network perimeter of corporate information systems. On average, in 27% of cases, professionals can not overcome the network perimeter and access the resources of the internal local area network. Since enterprise confidential information (e-mail, account passwords, server access details, hash data user accounts, and other information that is not publicly accessible) is the goal for many cybercriminals, these technologies are often become a subject of attacks. Thus, the problem of identifying and analyzing vulnerabilities in information security in corporate information systems is relevant to date. In conducting the analysis we relied on the study of foreign scientists and practitioners engaged in the study of threats and the development of their prevention systems. The study of this issue enables to identify and classify possible threats and modernize existing or develop new effective methods and measures of information security.

Keywords: corporate information systems, computer networks, threats of information security, information protection.

Мехед Дмитро Борисович, к.п.н., доцент кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Мехед Дмитрий Борисович, к.п.н., доцент кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Mekhed Dmytro, PhD, associate professor of the department of cybersecurity and mathematical simulation, Chernihiv National University of Technology.

Ткач Юлія Миколаївна, к.п.н., доцент, завідувач кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Ткач Юлия Николаевна, к.п.н., доцент, заведующая кафедрой кибербезопасности и математического моделирования Черниговского национального технологического университета.
Tkach Yulia, PhD, associate professor, head of the department of cybersecurity and mathematical simulation, Chernihiv National University of Technology.

Базилевич Володимир Маркович, к.е.н., доцент кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Базилевич Владимир Маркович, доцент кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Bazylevych Volodymyr, PhD, associate professor of the department of cybersecurity and mathematical simulation, Chernihiv National University of Technology.

Гур'єв Володимир Іванович, к.т.н., професор кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Гурьев Владимир Иванович, к.т.н., профессор кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Guriev Volodymyr, PhD, professor of the department of cybersecurity and mathematical simulation, Chernihiv National University of Technology.

Усов Ярослав Юрійович, асистент кафедри інформаційних та комп'ютерних систем Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Усов Ярослав Юрьевич, ассистент кафедры информационных и компьютерных систем Черниговского национального технологического университета.
Usov Yaroslav, assistant of the Department of Information and Computer Systems, Chernihiv National University of Technology.