УДК 004.056.5

А. О. Азарова
Ю. О. Оверченко
Л. М. Ткачук

ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ УКРАЇНСЬКИХ БАНКІВ ВІД КІБЕРНЕТИЧНИХ АТАК

Анотація

У роботі вивчено стан захищеності української банківської системи від кібернетичних атак хакерів. Обґрунтовано доцільність застосування системного підходу, який би примусив банківські структури використовувати комплексно систему програмних і апаратних засобів, які б дозволили забезпечити високий рівень захищеності своєї інфраструктури із збереженням достатньої ефективності бізнес-процесів. Доцільність впровадження такої системи є наявність ефектів синергії та емерджентності, які уможливлюють отримання додаткового системного ефекту, який виникає під час взаємодії двох чи більше компонентів системи, причому їх сукупна дія суттєво переважає суму впливів окремо взятих компонентів, а також появі особливих властивостей у системі елементів, не притаманних її підсистемам (апаратному чи програмному рівням захисту) або їх сумі. Запропоновано низку взаємопов'язаних елементів такої системи, що уможливлюють високий рівень захисту банківської сфери від кібератак.

Ключові слова: *кібератака, системний підхід, захист інформації, банківська сфера.*

Abstract

The paper deals with the state of security of the Ukrainian banking system against cyberattacks by hackers. The feasibility of applying a systematic approach that would force banking structures to use a comprehensive system of software and hardware to ensure a high level of security of their infrastructure while maintaining sufficient efficiency of business processes is substantiated. The feasibility of implementation of such a system is the presence of synergy and emergence effects which make it possible to obtain an additional system effect that occurs during the interaction of two or more components of the system and their combined action significantly outweighs the amount of effects of individual components, as well as the appearance of special properties in the system of elements, not inherent in its subsystems (hardware or software security levels) or their sum. A number of interconnected elements of such a system are offered, which allow a high level of protection of the banking sector against cyberattacks.

Keywords: *cyberattack, system approach, information security, banking.*

Вступ

Фінансові дані – один із найпопулярніших об'єктів атак кіберзлочинців в інформаційному просторі. Найбільш вигідні дані, використання яких спрямоване на отримання грошового прибутку, знаходяться у розпорядженні фінансових організацій. Саме через це банківські установи завжди знаходяться під загрозою кібернетичних атак на всіх рівнях своєї IT-інфраструктури у будь-якій точці світу.

Наявні методи захисту не є дієвими, про що свідчать постійні повідомлення про викрадення грошових коштів, розміщених у банках, та їх переведення на інші рахунки, шахрайські схеми заволодіння коштами фізичних та юридичних осіб, що є клієнтами банку та ін.

Отже, метою дослідження є аналіз захищеності банків України від кіберзлочинів та вироблення відповідних рекомендацій щодо підвищення рівня захищеності від кібератак.

Результати дослідження

Кібератакою (хакерською атакою) є замах на інформаційну безпеку комп'ютерної системи будь-якої організації. Особливої привабливості до замахів хакерів набули банківські послуги, оскільки вони є взаємопов'язаними, і з ланцюжка одиночних атак, які не становлять безпосередньої небезпеки в кожному окремому випадку, можна здійснити успішне проникнення

до критично важливої системи. Отже, слід зазначити, що навіть уразливість банківської комп'ютерної мережі в одному аспекті може бути використана зловмисником для успішної кібератаки на цілу організацію.

Однак, не зважаючи на те, що з кожним роком в Україні збільшується кількість кібератак, пов'язаних з отриманням фінансових даних і подальшим використанням їх кіберзлочинцями у власних цілях, близько половини українських банків і платіжних систем (48%) вважає за краще боротися з наслідками кібератак, а не інвестувати кошти у засоби для покращення рівня захисту даних і рахунків своїх клієнтів.

Автори вважають, що для вирішення таких проблем необхідно застосовувати системний підхід, який би примусив банківські структури використовувати комплексно цілу систему програмних і апаратних засобів, які б дозволили забезпечити високий рівень захищеності своєї інфраструктури із збереженням достатньої ефективності бізнес-процесів. Сенсом впровадження такої системи є наявність ефектів синергії та емерджентності.

Ефект синергії (від гр. *συνεργία* − співпраця, *σύν* − разом, *έργον* − дія) полягає у додатковому системному ефекті, який виникає під час взаємодії двох чи більше компонентів системи, причому їх сукупна дія суттєво переважає суму впливів окремо взятих компонентів. Розглянемо отримані перспективи у розв'язку поставленої задачі від появи такого системного явища, як синергії:

- користь окремо від програмних або апаратних засобів захисту інформації є значно меншою, доки їх не застосовано разом;
- з'єднання двох або більше підходів спричиняє додатковий ефект, який суттєво перевищує просте підсумовування ефектів від кожного з окремо взятих засобів.

Другим позитивним чинником, що сприяє розв'язку проблем захисту банківської системи на основі застосування системного підходу, є емерджентність – поява особливих властивостей у системі елементів, не притаманних її підсистемам (апаратному чи програмному рівням захисту) або їх сумі; неможливість зведення властивостей системи до суми властивостей її компонентів.

Отже, розглянемо низку таких взаємопов'язаних між собою елементів системи захисту банківських ресурсів.

1) для протистояння атакам ефективними є методи соціальної інженерії – це регулярне навчання всіх співробітників компанії безпечній роботі в Інтернет-мережі та інформування їх про існуючі види загроз;

2) усі торгові точки, на яких може використовуватися пластикова карта будь-якого банку, є потенційно уразливими об'єктами доти, доки їх POS-термінали не захищені спеціалізованим програмним забезпеченням;

3) користування послугами сторонніх компаній, які спеціалізуються на захисті даних від DDoS-атак, підключившись до хмарних сервісів організації;

4) сайтам, яким найбільше загрожують кібератаки, слід уважніше ставитися до рівня своєї безпеки. Необхідно посилити захищеність від підбору ідентифікаторів або паролів користувачів. Слід зазначити, що найнебезпечніші сайти написані мовою PHP, оскільки 76% з них містять критичні уразливості. Менш уразливими виявилися веб-ресурси, написані мовою Java (70%) і ASP.NET (55%) (згідно даних компанії Positive Technologies);

5) адміністратори корпоративної мережі організації повинні контролювати, якими додатками користуються співробітники і які сайти вони відвідують. У них повинні бути дійсні сертифікати SSL.

Висновки

Інформаційна безпека та захист інформації банку мають бути системними, для того щоб відбивати будь-які хакерські атаки і спроби будь-яких вторгнень з боку кіберзлочинців, у тому числі з боку співробітників самої організації. Для того, щоб мінімізувати фінансові, а в подальшому й репутаційні ризики, службам безпеки банків необхідно захищати не лише бази даних і робочі станції персоналу, а також і комп'ютерні мережі, термінали працівників фронт-офісу та банкомати небезпечних кодів і дій кіберзлочинців.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навчальний посібник. Вінниця : ВНТУ, 2017. 120 с.

2. Азарова А. О., Желюк Н. С. Вибір, планування та реалізація стратегії розвитку підприємства. *Актуальні проблеми економіки*. №12. 2010. С. 91–100.
3. Азарова А. О., Гаврилова О. В. Розробка методики визначення економічної безпеки підприємства. *Економіка: проблеми теорії та практики*. Дніпропетровськ : ДНУ, 2004. Вип.191, т. ІІІ. С. 719–727.
4. Азарова А. О., Антонюк О. В. Математичні моделі оцінювання стратегічного потенціалу підприємства та прийняття рішень щодо його підвищення. Вінниця : ВНТУ, 2012. 168 с.
5. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М. : Радио и связь, 2001. 376 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.
7. Азарова А. О., Ткачук Л. М., Шиян А. А., Нікіфорова Л. О., Хошаба О. М. Публічне управління та адміністрування в контексті захисту його інформаційного простору. *Вісник Житомирського державного технічного університету*. 2019. № 2. С.149–155.
8. Азарова А.О., Мисько Ю. О., Сембрат Д. С. Розробка програмних модулів ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією. Тези XLVII науково-технічної конференції ВНТУ. 2018. URL: https://ir.lib.vntu.edu.ua/handle/123456789/22446.
9. Азарова А. О., Гудзь В. О., Блонський В. О. Управління та адміністрування захистом інформації шляхом локалізації закладних пристроїв на основі індитикатора електромагнітних випромінювань. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7335/6122
10. Азарова А. О., Гудзь В. О., Блонський В. О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7429
11. Азарова А. О., Чайковська Я. В. Вдосконалення методу вбудовування цифрових водяних знаків на основі квантування для підвищення рівня захисту PDF файлів. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7828
12. Азарова А. О., Хісматулліна В. Ф. Електронні засоби політики інформаційної безпеки на державних підприємствах. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/6889.
13. Азарова А.О., Азарова Л. Є., Ткачук Л.М., Шиян А. А., Нікіфорова Л. О., Кудлик А. В. Комп'ютерна програма «Модуль захисту програмного забезпечення від несанкціонованого копіювання у процесах публічного управління». Свідоцтво про реєстрацію авторського права на твір №90163 від 25.06.19 р. Заявка №91534 від 10.06.2019 р.
14. Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації". Свідоцтво про реєстрацію авторського права на твір №79708. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
15. Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Свідоцтво про реєстрацію авторського права на твір №79707. Розробка контролеру кодового доступу до сейфа на мікроконтролері Arduino. Заявка від 05.06.2018 р. №80960. Дата реєстрації 14.06.2018 р.
16. Азарова А. О., Азарова Л. Є., Бадя Ю. В. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах". Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
17. Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.

Азарова Анжеліка Олексіївна – к.т.н., проф. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м. Вінниця, e-mail: azarova.angelika@gmail.com.
Оверченко Юрій Олегович – студент гр. УБ-19М факультету менеджменту та інформаційної безпеки, м. Вінниця, e-mail: yuraoverchenkoub@gmail.com
Ткачук Людмила Миколаївна – к.е.н., доц. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з навчально-методичної роботи Вінницького національного технічного університету,м. Вінниця, e-mail: ludatkachuk2017@gmail.com.

Azarova Anzhelika O. — PhD in technique, Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.
Overchenkj Yurii O. – Department of management and security of information systems, Vinnytsia National Technical University, Vinnytsia.
Lyudmila Tkachuk – PhD in economic, Assistant Professor, Deputy dean of the Faculty of management and information security by educational work of Vinnytsia National Technical University, Vinnytsia, email : ludatkachuk2017@gmail.com