

УДК 336.76

ШАМОВ Сергій Олександрович,
кандидат технічних наук, доцент,
Харківський навчально-науковий інститут
ДВНЗ «Університет банківської справи»,
м. Харків, Україна
САРБАШ Альона Олександрівна,
студентка, Харківський навчально-науковий
інститут ДВНЗ «Університет банківської справи»,
м. Харків, Україна

ЗАГРОЗИ ДІЯЛЬНОСТІ БРОКЕРСЬКИХ КОМПАНІЙ

Робота присвячена проблемі захисту діяльності брокерських компаній на фінансових ринках від зовнішніх загроз, реалізація яких призводить до великих фінансових втрат і істотно знижує ефективність їх діяльності. Проведено аналіз загроз діяльності брокерських компаній на ринку Forex, типових наслідків від їх реалізації, властивих і можливих шляхів захисту від них засобами інформаційних технологій. Виділено три найбільш значущі глобальні загрози, характерні для сучасного стану фінансових ринків і світової економіки в цілому. Показана їх обумовленість ключовою роллю комп'ютеризованих інформаційних технологій у сучасному бізнесі та нестримним бурхливим розвитком засобів здійснення злочинної діяльності у комп'ютерному інформаційному просторі. Розглянуті запропоновані ІТ компаніями програмні та технічні засоби, що дозволяють ефективно протидіяти цим загрозам. Запропоновано склад системи таких засобів для захисту діяльності брокерських компаній на фінансових ринках.

Ключові слова: ринок Forex, брокерські компанії, валюта, кібератаки, інформаційні технології, загрози.

Постановка проблеми. Ринок Forex – наймасштабніший сегмент світової фінансової індустрії, це всесвітній віртуальний простір, де працюють банки, інвестиційні та пенсійні фонди, страхові компанії, брокерські фірми і мільйони приватних інвесторів. Тут щоденно змінюються рівні попиту і пропозиції, ціни і наміри учасників ринку. Щоденний оборот валютного ринку Forex – близько \$ 4 трильйонів.

З великими грошима завжди пов'язані великі ризики, наявність яких обумовлює актуальність і гостроту проблеми забезпечення безпеки і ефективності торговельної діяльності на фінансових ринках.

Аналіз останніх досліджень і публікацій. Однією з найважливіших задач, що необхідно розв'язувати кожному учаснику фінансового ринку, є вибір брокера, а разом з ним і умов для виходу на ринок, який ґрунтується на багатоаспектному аналізі [1]:

- наявності і особливостей офіційної реєстрації;
- відгуків інших учасників ринку;
- якості сервісу і партнерської програми;
- зручності, функціональності, надійності та безпечності програмного забезпечення, що надається клієнту і використовується брокером;
- ставлення брокера до скарг (швидка реакція, допомога і консультація – відмінні риси надійного брокера);
- надійності процесів введення і виведення коштів учасника торгівлі (клієнта брокера).

Якщо у брокера є центові рахунки, буде доцільно перевірити роботу системи: внести пару доларів, а потім їх зняти. У надійних брокерів відсутні перешкоди для зняття грошових коштів.

У рейтингу Forex-брокерів в країнах СНД по надійності в 2015-2016 роках лідирує Forex-брокер Alpari (торгові платформи: MetaTrader 4, MetaTrader 5). Він є прикладом надійності, солідності і просто досвідченого Forex-брокера. Друге місце займає Alfa-forex (торгові платформи: MetaTrader 4, MetaTrader 5, ActTrader, Zulutrade, мобільні додатки). На третьому місці розташувався Dukascopy (торгова платформа: JForex, Java, Web-

платформа, SWFXTrader для AppleiOS, SWFXTrader для Android) [2, 3]. Всі вони – взірці доброї репутації і компетентності. Однак, необхідно зазначити, що існують загрози, які не дивлячись на успішність і надійність компанії можуть завдати їй непоправної шкоди.

Оскільки вся діяльність сучасних брокерів здійснюється в кіберпросторі з використанням всього спектру сучасних комп'ютерних засобів, засобів телекомунікації та програмного забезпечення, наявність таких загроз є викликом для ІТ-компаній, які виробляють ці засоби. Удосконалення засобів ІТ для фінансових ринків є одним з актуальних і популярних напрямів бізнесу ІТ компаній, що достатньо широко висвітлене в публікаціях, наприклад [4]. Однак у науковій літературі вказаній проблемі поки не приділяється достатньо уваги, номенклатура програмних засобів для брокерів багато років залишається фактично незмінною, що піддає все більшій небезпеці благополуччя не тільки брокерів, а й світової фінансової системи в цілому.

Мета та завдання дослідження. Виходячи з цього **метою статті** є аналіз загроз діяльності брокерських компаній і можливих шляхів захисту від них засобами інформаційних технологій. **Завданням статті** є пошук систем засобів інформаційних технологій, що дозволять ефективно протидіяти реалізації виникаючих загроз та ризиків.

Виклад основного матеріалу дослідження. Аналіз публікацій показав, що в даний час найбільшу небезпеку брокерської діяльності уявляють, перш за все, глобальні загрози, які можуть мати негативний вплив на Forex-індустрію в цілому.

Загроза 1. Коливання курсу національної валюти. Проблема полягає в тому, що падіння курсу національної валюти може знецінити активи Forex-компаній, і вони вже не зможуть забезпечувати виплати клієнтам в повній мірі [5].

Прикладом такої проблеми є нестабільність офіційного курсу гривні, що відображена на діаграмі (рис. 1) за даними Національного банку України [6].

Причиною таких падінь курсу, на думку фінансистів, є незначна пропозиція валюти з боку Національного банку України, який прагне зберігати обсяги своїх резервів до моменту отримання чергового кредитного траншу від МВФ [7].

Рішенням проблеми коливання курсу може бути прогнозування рівня інфляції, адже повідомлення про підвищення рівня інфляції викликають різке падіння курсу, якщо ж йдеться про падіння цін на основні товарної групи, на ринку утворюється висхідний тренд. Для цього можна запропонувати декілька інструментів. Одним з них є автоматичне оновлення курсів валют в MS Excel за допомогою функцій Вебслужба і Фільтр.XML [8].

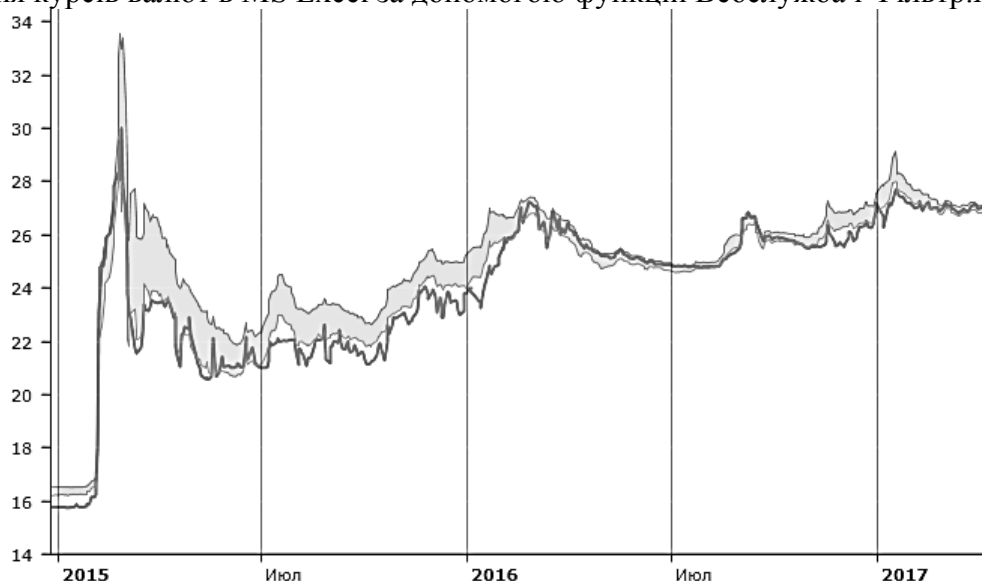


Рис. 1. Курс USD/UAH [6]

Також, на сайтах брокерів ринку Forex відбувається постійне оновлення котирувань по всіх валютних парах. Для андроїд пристроїв, існує додаток «Курси валют НБУ (віджет)». Це

єдиний віджет для відображення курсів валют Національного банку України. Інформація оновлюється тільки після натискання, таким чином, економлячи трафік [9].

Загроза 2. Кібератаки. Увага кіберзлочинців до фінансових компаній зростає щодня. Фахівці відомого розробника антивірусного програмного забезпечення «Лабораторія Касперського» стверджують, що в другому кварталі 2016 року антивірусне ПЗ заблокувало понад мільйон фінансових вірусів [10]. Останнім часом спостерігається об'єднання зусиль розробників шкідливих програм, а спеціалізовані трояни для злову сайтів банків і фінансових компаній стають головною і найбільш небезпечною кіберзагрозою. Найбільш помітною стала співпраця розробників Gozi і Nymaim – двох найбільш відомих банківських троянських програм. Так початкова версія троянської програми Nymaim розроблялась як інструмент для здирництва, шляхом блокування доступу користувачів до необхідної інформації і вимагання винагороди за його розблокування. У подальшому результатом співпраці двох компаній стали версії, що мають функціонал, запозичений у іншій троянській програмі – Gozi, який забезпечує шахраям можливість віддаленого доступу до комп'ютерів, що є об'єктами атаки. В якості лідера серед шкідливого програмного забезпечення, спрямованого проти Інтернет-ресурсів фінансових установ, фахівці називають програми сімейства Zbot, на частку яких припадає близько 16% всіх заблокованих антивірусними програмами кібератак [11].

Проведений аналіз антивірусних засобів показав, що таким кібератакам можна ефективно протидіяти за допомогою наступних програм:

1) Network Defense – спеціалізована платформа безпеки, здатна в масштабах всієї мережі виявляти шкідливі програми «нульового дня», підозрілий обмін даними і атакуючі дії, непомітні для традиційних систем захисту. Вона запускає підозрілий код в безпечних контрольованих умовах, які можуть бути оптимізовані і налаштовані для підвищення продуктивності і захисту системи від методів злову, орієнтованих на ізольовані середовища [12];

2) X-ForceExchange – платформа, що містить величезні обсяги узагальненої інформації про загрози, рекомендації, практично реалізовані в IBM і інших компаніях по всьому світу, а також індикатори атак в режимі реального часу [13];

3) Zillya – програма, що здатна захистити брокерське програмне забезпечення від вірусів, троянських та шпигунських програм, руткітів, рекламних програм, а також досі не реалізованих загроз за допомогою інтелектуального модулю про активного захисту. Він здатен визначати вірусне походження програм незалежно від наявності попередньої інформації про їх шкідливість та знешкоджувати їх. Основою такого захисту даних від усіх типів шкідливих програм є база знань, яка вміщує понад 15 мільйонів вірусних сигнатур та оновлюються щоденно [11].

4) Пристрої Siprotec від Siemens – потужне і досконале поєднання мікропроцесорних пристроїв захисту і керування, які можуть застосовуватися на електричних підстанціях будь-якого класу напруг. Таким чином, використання мікропроцесорних пристроїв управління та релейного захисту лінійки Siprotec дозволять побудувати електричну підстанцію з багаторівневим керуванням та захистом від помилок персоналу та від зовнішнього втручання [14]. Перевагами пристрою Siprotec є:

- *надійність та тривалий термін експлуатації.* Більше ніж 20 років компанія Siemens займається проектуванням та виготовленням цифрових захистів, тому у пристрої використовується надійна мікропроцесорна техніка. А використання великих інтегральних мікросхем дозволило скоротити чисельність електронних елементів;
- *наявність додаткових захисних функцій.* Ці функції передбачають захист від перевантаження, фазно-струмовий захист та захист від теле-відключення;
- *резервний захист.* Він дозволяє уникнути істотних пошкоджень обладнання на підстанціях при аварійних режимах в разі неспрацьовування основних захистів;
- *вивід повідомлень із зазначенням часу.* Пристрій проводить реєстрацію аварійних подій з виводом робочих повідомлень [15].

Загроза 3. Панічні настрої на фінансових ринках. Їх небезпеку наочно демонструють наступні приклади.

Рішення Swiss National Bank відмовитися від прив'язки своєї національної валюти до євро призвело в 2015-2016 роках до безладу на ринку Forex і непередбачуваних хаотичних змін обмінних валютних курсів, у першу чергу для валютної пари EUR/CHF. Фінансові втрати брокерської спільноти навіть на початку цього процесу склали понад один мільярд доларів [16].

Наслідком виходу Великобританії з ЄС стало стрімке та максимальне за всю його історію існування падіння британських фондових індексів: FTSE 250 – понад 11%, а FTSE 100 – 8%.

Подібні «круті» політичні та економічні рішення, що почастишали в останні роки, щоразу викликають на фінансових ринках ефект доміно, і в решті решт паніка охоплює інвесторів в усьому світі. Так сумнозвісний «Brexit», підтверджуючи свою зловісну назву (від англійського «breaks it» або «BRitain+EXIT», що найчастіше перекладається як пошкодити, зруйнувати, порушити), викликав падіння всіх основних фондових індексів: японського TOPIX – на 7,3%, французького CAC40 – на 9,2%, німецького DAX – на 8,2%, італійського FTSE MIB – на 10,6%, іспанського IBEX 35 – на 10,26%, загальноєвропейського The Stoxx Europe 600 – на 6,6%, російських ММВБ та РТС – на 2,64% та 4,48% (станом на 09:00, 24.06.2016 р. за Гриневичем) [17]. Ринки сировини також негайно відреагували: ціна нафти впала до рівня USD 48,30 за барель [18].

Хоча такі різкі зміни таять в собі велику небезпеку, в принципі коливання котирувань – звичайне явище для фінансових ринків. Спрогнозувати коливання котирувань допоможе технічний аналіз, який є невід'ємною частиною інструментів для моніторингу коливання котирувань базових активів. Серед важливих інструментів цього аналізу особливе місце займають технічні індикатори – статистичні функції, що ґрунтуються на припущенні, що всі цінові зміни мають закономірний характер. Одним з найбільш популярних, вважається індикатор Stochastic, який показує стан ціни щодо діапазону цін за встановлений період в минулому і відображається в процентах [19]. Йому, за значимістю не поступається і індикатор RSI, який слугує для визначення сили поточного цінового тренду, і який порівнює абсолютну величину зростання ціни за певний проміжок часу з рівнем її падіння за той же період. Результати розрахунків зазвичай виводяться користувачеві на екран торговельного терміналу у вигляді кривої на курсовому графіку, з діапазоном значень від 0 до 100% [20]. Постійне використання цих інструментів, на наш погляд, дозволить брокерам своєчасно реагувати на виникаючі загрози.

Висновки та перспективи подальших розвідок. В результаті дослідження загроз діяльності брокерських компаній запропонована система засобів інформаційних технологій, що дозволяє ефективно протидіяти реалізації виникаючих ризиків. Застосування програм Network Defense, X-Force Exchange, Zillya дозволить відстежити і провести аналіз проблем антивірусного захисту, використовуючи інформацію з різних джерел, включаючи власні бази даних, а також дає можливість попереджувати вплив сучасних спеціалізованих атак. Пристрої Siprotec від Siemens миттєво відстежують несправності, розпізнають та усувають їх. Застосування програм Вебслужба і Фільтр.XML дає можливість простежити зростання і падіння курсів валюти. Встановлено, що для виявлення ризиків, пов'язаних з коливаннями котирувань, варто використовувати технічні індикатори Stochastic і RSI.

В решті вважаємо за потрібне наголосити на гострій актуальності проблеми кібернетичного захисту інформаційних систем, що функціонують на фінансових ринках всього світу і необхідності зосередження зусиль як фахівців-практиків так і науковців у галузі інформаційних технологій на її розв'язанні.

Список використаних джерел

1. Форекс брокери – как правильно выбрать брокера Forex + рейтинг ТОП-10 лучших компаний по надежности (с лицензией ЦБ РФ). [Електронний ресурс] / Фінансовий журнал «Richpro.ru». – Режим доступу: <http://richpro.ru/finansy/foreks-brokerov-rejting-luchshih-forex-brokerov.html>.

2. Торговля на валютном рынке Forex и форекс брокеры. [Электронный ресурс] / BalanceFinance. – Режим доступа: <http://balancefinance.com>.
3. Форекс брокер Рейтинг – лучший рейтинг брокеров Forex. [Электронный ресурс] / Рейтинг брокеров Форекс. – Режим доступа: <http://forex-ratings.ru/>.
4. Кирилл Жабин Риски информационной безопасности финансового рынка. Прогноз 2017. [Электронный ресурс] / Информзахист. Системный интегратор. – Режим доступа: <http://www.infosec.ru/news/experts/9892>.
5. Новости в Украине и мире. Последние новости ТСН. [Электронный ресурс] / ТСН. – Режим доступа: <https://ru.tsn.ua/>.
6. FinStat. Курс гривны к доллару, динамика (НБУ, наличный курс). [Электронный ресурс] / FinStat. – Режим доступа: <https://finstat.info/dinamika-kursa-dollar-ssha-nbu-nalichnyiy-kurs>.
7. Обреченный курс. Почему гривна продолжит падать. [Электронный ресурс] / РІА Новини Україна. – Режим доступа: <http://rian.com.ua/view/20160202/1004558811.html>.
8. Импорт курса валют из интернета. [Электронный ресурс] / Планета Excel. – Режим доступа: <http://www.planetaexcel.ru/techniques/11/129/>.
9. Лучшие отечественные android-приложения курсов валют. [Электронный ресурс] / Mobile Review. – Режим доступа: <http://android.mobile-review.com/%20market/7255/>.
10. Кибератаки – реальная угроза для финансового сектора. [Электронный ресурс] / Forex Magnates. – Режим доступа: <http://ru.forexmagnates.com/kiberataki-realnaya-ugroza-dlya-finansovogo-sektora/>.
11. Zillya – максимальный захист від існуючих кіберзагроз. [Электронный ресурс] / Антивірус Zillya. – Режим доступа: <http://zillya.ua/>.
12. Кибератаки и их жертвы. [Электронный ресурс] / Безпека в Інтернеті. – Режим доступа: <http://security.mosmetod.ru/moshennichestvo-v-seti/58-kiberataki>.
13. IBM представляет новое решение для борьбы с кибератаками. [Электронный ресурс] / Хабрахабр. – Режим доступа: <https://habrahabr.ru/company/ibm/blog/257783/>.
14. Компания Siemens защищает украинцев от кибератак. [Электронный ресурс] / 24 канал. – Режим доступа: http://24tv.ua/kompaniya_ziemenz_zahishhaye_ukrayintsiv_vid_kiberatak_n802278.
15. Siemens Siprotec – захист обладнання та управління ним в одному пристрої. [Электронный ресурс] / Allremont. – Режим доступа: <http://allremont.com/article/-/siemens-siprotec-zaschita-oborudovaniya-i-upravlenie-im-v-odnom-ustrojstve>.
16. Брекзит – новая возможность или угроза для отрасли? [Электронный ресурс] / Forex Magnates. – Режим доступа: <http://ru.forexmagnates.com/brekzit-novaya-vozmozhnost-ili-ugroza-dlya-otrasli/>.
17. Выход Британии из ЕС: что это значит для нас всех. [Электронный ресурс] / Дождь. – Режим доступа: <https://tvrain.ru/articles/brexit-412017>.
18. Брекзит – смелый и необдуманный шаг Великобритании. [Электронный ресурс] / Інвестиції в Інтернеті «Profvest». – Режим доступа: <http://www.profvest.com/2016/07/brexit-posledstviya.html>.
19. Технический метод прогнозирования колебания котировок. [Электронный ресурс] / Російський брокер бінарних опціонів «Binex». – Режим доступа: <https://binex.ru/ru/training/strategies/tehnicheskij-metod-prognozirovaniya-kolebaniya-kotirovok.html>.
20. Как правильно применять технический индикатор RSI. [Электронный ресурс] / ВсемПроблемам.Нет. – Режим доступа: <http://vsemproblemam.net/trading-tools/kak-pravilno-primenjat-indikator-rsi.html>.

References

1. Financial magazine «Richpro.ru». *Forex brokers – how to choose the right Forex broker + rating TOP-10 of the best reliability companies (with the license of the CBR)*. [Electronic resource]. – Access mode: <http://richpro.ru/finansy/foreks-brokeroy-rejting-luchshih-forex-brokerov.html>.
2. BalanceFinance. *Forex trading and Forex brokers*. [Electronic resource]. – Access mode: <http://balancefinance.com>.
3. Forex Brokers Rating. *Forex Broker Rating – the best rating of Forex brokers*. [Electronic resource]. – Access mode: <http://forex-ratings.ru/>.
4. Cyril Zhabin. Information protection. System integrator. *Risks of information security of the financial market. Forecast 2017*. [Electronic resource]. – Access mode: <http://www.infosec.ru/news/experts/9892>.
5. TSN. *News in Ukraine and in the world. Latest TSN news*. [Electronic resource]. – Access mode: <https://ru.tsn.ua/>.
6. FinStat. *The rate of the hryvnia to the dollar, dynamics (NBU, cash rate)*. [Electronic resource]. – Access mode: <https://finstat.info/dinamika-kursa-dollar-ssha-nbu-nalichnyiy-kurs>.
7. RIA News of Ukraine. *Doomed course. Why the hryvnia will continue to fall*. [Electronic resource]. – Access mode: <http://rian.com.ua/view/20160202/1004558811.html>.
8. Planet Excel. *Importing exchange rates from the Internet*. [Electronic resource]. – Access mode: <http://www.planetaexcel.ru/techniques/11/129/>.
9. Mobile Review. *Best domestic currency android-application*. [Electronic resource]. – Access mode: <http://android.mobile-review.com/%20market/7255/>.
10. Forex Magnates. *Cyberattacks are a real threat to the financial sector*. [Electronic resource]. – Access mode: <http://ru.forexmagnates.com/kiberataki-realnaya-ugroza-dlya-finansovogo-sektora/>.

11. Antivirus Zillya. *Zillya – maximum protection of existing cyber threats*. [Electronic resource]. – Access mode: <http://zillya.ua/>.
12. Internet Security. *Cyberattacks and their victims*. [Electronic resource]. – Access mode: <http://security.mosmetod.ru/moshennichestvo-v-seti/58-kiberataki>.
13. HABRAHABR. *IBM is introducing a new solution to combat cyberattacks*. [Electronic resource]. – Access mode: <https://habrahabr.ru/company/ibm/blog/257783/>.
14. 24th channel. *Siemens is protected by Ukrainian cyberattacks*. [Electronic resource]. – Access mode: http://24tv.ua/kompaniya_ziemenz_zahishhaye_ukrayintsiv_vid_kiberatak_n802278.
15. Allremont. *Siemens Siprotec – equipment protection and management in one device*. [Electronic resource]. – Access mode: <http://allremont.com/article/-/siemens-siprotec-zaschita-oborudovaniya-i-upravlenie-im-v-odnom-ustrojstve>.
16. Forex Magnates. *Is Brexite a new opportunity or a threat to the industry?* [Electronic resource]. – Access mode: <http://ru.forexmagnates.com/brekzit-novaya-vozmozhnost-ili-ugroza-dlya-otrasli/>.
17. Rain. *The exit of Britain from the EU: what does this mean for us all*. [Electronic resource]. – Access mode: <https://tvrain.ru/articles/brexit-412017>.
18. Investments in Internet «Profvest». *Brexit is a brave and rash step of Great Britain*. [Electronic resource]. – Access mode: <http://www.provest.com/2016/07/brexit-posledstviya.html>.
19. Russian binary options broker «Binex». *Technical method of forecasting the fluctuation of quotations*. [Electronic resource]. – Access mode: <https://binex.ru/ru/training/strategies/tehnicheskij-metod-prognozirovaniya-kolebaniya-kotirovok.html>.
20. VsemProblemam.Net. *How to apply the technical indicator RSI correctly*. [Electronic resource]. – Access mode: <http://vsemproblemam.net/trading-tools/kak-pravilno-primenjat-indikator-rsi.html>.

SHAMOV Sergii Oleksandrovyh,

Candidate of Technical Sciences, assistant professor,
Kharkiv Educational and Scientific Institute
of SHEI «Banking University»;

SARBASH Alyona Oleksandrivna,

Student, Kharkiv Educational and Scientific Institute
of SHEI «Banking University»

THREATS FOR ACTIVITIES OF BROKER COMPANIES

Abstract. Introduction: *The article devoted to the protection of activities of broker companies in financial markets from external threats, realization of which results in large financial losses and significantly reduces the efficiency of their activities.*

Purpose: *Research purpose is an analysis of threats to activities of broker companies and possible ways to protect them by means of information technology.*

Methods: *monitoring, system analysis, induction, generalization.*

Results: *In this article the analysis of such threats in the market Forex, typical consequences of their realization, typical and possible ways to protect them by means of information technology. Three most significant global threats is characteristic of the modern state of financial markets and the world economy as a whole. Was shown their dependence key role of computerized information technologies in the modern business and uncontrollable rapid development of tools for criminal activities in computer information space. IT companies considered the proposed program and technical tools to effectively combat these threats.*

Originality: *is in the formulation and offering solutions to problems identifying opportunities for creating a system of information technology to protect brokerage activities in financial markets on a combination of the most significant global threats caused by a combination of global computerization of such activities with the rapid development of computer crime in information space.*

Conclusion: *Proposed composition of systems tools to protect activities of broker companies in the financial markets, which tools and their uses discussed in this article. The problem of cyber protection information systems, that operate in the financial markets around the world and the need to concentrate efforts both practicing specialists and researchers in the field of information technology to solve it, is important and actual.*

Keywords: *market Forex, broker companies, currency, cyberattacks, information technology, threats.*

Одержано редакцією: 28.04.2017
Прийнято до публікації: 10.05.2017