УДК 330.654

Сотниченко В.М.
кандидат педагогічних наук, доцент,
завідувач кафедри підприємництва,
торгівлі та біржової діяльності
Державного університету телекомунікацій

ВПЛИВ ТЕХНІКО-ТЕХНОЛОГІЧНОЇ СКЛАДОВОЇ НА СТАН ЕКОНОМІЧНОЇ БЕЗПЕКИ

У статті розглянуто питання захисту відкритих комп'ютерних мереж як запоруки економічної безпеки підприємства. Надано коротку характеристику наявних систем захисту. Висвітлено перспективи їх розвитку. Наголошено на необхідності поглиблення знань керівників підприємств сучасних засобів захисту інформації і вдосконалення прийомів та методів забезпечення економічної безпеки на техніко-технологічному рівні.

Ключові слова: адаптивна система захисту, інформаційна безпека, економічна безпека, відкриті комп'ютерні мережі, кіберпростір.

Сотниченко В.Н. ВЛИЯНИЕ ТЕХНИКО-ТЕХНОЛОГИЧЕСКОЙ СОСТАВЛЯЮЩЕЙ НА СОСТОЯНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В статье рассматриваются вопросы защиты открытых компьютерных сетей как залога экономической безопасности предприятия. Предоставляется краткая характеристика существующих систем защиты. Освещаются перспективы их развития. Отмечается необходимость углубления знаний руководителями предприятий современных средств защиты информации. Совершенствование приемов и методов обеспечения экономической безопасности на технико-технологическом уровне.

Ключевые слова: адаптивная система защиты, информационная безопасность, экономическая безопасность, открытые компьютерные сети, киберпространство.

Sotnychenko V.N. INFLUENCE TEHNIKO-TECHNOLOGICAL COMPONENT OF THE STATE OF ECONOMIC SECURITY

The article deals with the protection of open computer networks as a guarantee of economic security. Provided a brief description of the existing protection systems. Highlights the prospects of their development. The necessity of deepening the knowledge of business leaders of modern means of information protection. Improving the methods and techniques of economic security on the technical and technological level.

Keywords: adaptive protection system, information security, economic security, public computer networks, cyberspace.

На сьогодні все більше дослідників у галузі економічної безпеки цікавляться адаптивною системою захисту систем і мереж. Це є досить цікавим предметом дослідження. Адаптивна система як система автоматичного управління зберігає працездатність в умовах непередбаченої зміни властивостей керованого об'єкту, цілей і завдань управління або умов навколишнього середовища за допомогою зміни алгоритмів свого функціонування або ж пошуку оптимальних станів. Таке визначення дає Велика радянська енциклопедія (третє видання), том. 22.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Масове застосування Інтернет-технологій у всіх галузях життєдіяльності людини, суспільства і держави є явищем звичним і закономірним. За допомогою ІТ-технологій вирішується практично весь комплекс завдань у соціально-економічній та оборонній сфері. І від того наскільки надійно захищені мережі передачі даних залежить економічна безпека суб'єктів господарювання. Сьогодні надзвичайно актуальним є володіння інформаційними технологіями, чітким уявленням про структуру і принципи побудови мереж. В економічній сфері діяльності без цього просто неможливо обійтися. Обізнаність у цьому важливому питанні допоможе більш ефективно захистити бізнес, посилити економічну безпеку підприємства.

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання цієї проблеми і на які спирається автор. Питанням володіння інформаційно-комунікаційними технологіями в бізнесі приділяє у своїх роботах В. Вишнівський [3]. В. Шевченко висвітлює у своїх дослідженнях кращий вітчизняний і світовий досвід управління інформаційною безпекою та її вплив на стабільність держави [12]. Більш докладно зупинився на спеціальних інформаційних операціях в економічному протиборстві

В. Петрик [9]. Зважуючи на значення інноваційних рішень в економіці на сучасному етапі її розвитку, системного моніторингу рівня підприємства, доречно звернутися до результатів досліджень О. Гудзь [6], Б. Бордмана [2]. Досвід щодо захисту обчислювальних систем із високим ступенем надійності тривалий час забезпечували такі традиційні механізми як ідентифікація й аутентифікація. Використовувалися такі методи як розмежування доступу і шифрування. Але з розвитком відкритих комп'ютерних мереж ситуація починає змінюватися. Збільшується кількість вразливостей мережевих операційних систем, різних прикладних програм, програмно-апаратного забезпечення. Це питання знайшло відображення в дослідженнях О. Лукацького [7; 8], В. Толубко [11]. У своїх роботах, вказані вище автори, виходили з погляду розгляду проблем на основі відкритих мереж.

До відкритої комп'ютерної мережі може приєднатися будь-яка особа, яка має відповідне обладнання. На шляху від відправника до отримувача пакети даних можуть бути втрачені, пошкоджені. Це представляє пряму загрозу для економічної безпеки підприємства, яку відображено в роботах В. Аврамова і С. Клименко [1], В. Гранатурова і Ю. Тараненка [4; 5]. Крім того, допускається і можливість створення зловмисниками своїх продуктів, призначенням яких може бути реалізація деструктивних функцій із метою викрадення ресурсу або прямого пошкодження системи. Це питання гостро стояло на парламентських слуханнях у Верховній Раді України 3 лютого 2016 р.

Для більш повного уявлення щодо актуальності дослідження проблеми, треба враховувати важливі

моменти, на які слід звернути увагу. По-перше, це те, що відкриті мережі самі постійно знаходяться під загрозою. По-друге, відкрита мережа – це транспортна система, якою шкідливий продукт буде доставлений до отримувача даних. Мережева безпека потребує до себе серйозної уваги в плані забезпечення економічної безпеки підприємства. Адміністратори безпеки мають мало часу для виявлення загроз, їх аудиту і класифікації, побудови адекватної системи захисту і знищення виявлених загроз.

Виділення невирішених раніше частин загальної проблеми, котрим присвячена означена стаття. Питання економічної безпеки здебільшого розглядають на платформі критеріїв, вироблених для захисту фізичної безпеки: розмежування доступу до об'єкту інтересів зловмисника, класифікація загроз, спостереження за допомогою спеціального обладнання, щоб не допустити фізичного вторгнення на об'єкт. Фізичний аспект безпеки не можна виключати із засобів боротьби проти загроз. Але вже сьогодні кожен підприємець, керівник виробництва повинен розуміти і робити з цього висновки на високопрофесійному рівні, що комп'ютерна безпека орієнтована на кіберпростір, де діють зовсім інші технології виявлення злочинців. І на цьому рівні економічна безпека ніяк не може бути гарантовано захищеною державою.

Законодавча база розроблена недостатньо, оскільки інформаційні технології ще не стандартизовані на такому рівні, щоб їх можна було прив'язати до сучасних юридичних норм. Кіберпростір не має кордонів, а розвиток законодавчої бази на порядки відстає від розвитку інформаційних і телекомунікаційних технологій. Це особливо актуально для України.

Атака може бути здійснена з будь-якої точки кіберпростору. Як приклад можна привести серію хакерських атак у листопаді 2016 р. на сервери російських банків, таких як Ощадбанк і Альфа-банк. Атаки було організовано з десятків тисяч машин, розташованих у 30 країнах світу, серед яких США, Індія, Тайвань, Ізраїль тощо. Середня тривалість атак – від однієї до майже дванадцяти годин. А потужність сягала 660 тисяч запитів за секунду.

Наведені дані є прикладом масштабного замаху на економічну безпеку, а щодо інших прецедентів, то їх маса. Зловмисники можуть читати нашу пошту, отримувати доступ до конфіденційної інформації (маркетингові і бізнес-плани), можуть впливати на фінансові дані і змінювати їх. Кіберзлочинці залишаються при цьому невидимими, важкодоступними для правоохоронної та судової системи.

Формулювання цілей статті (постановка завдання). Виходячи з вищенаведеного, обізнаність та підтримка прийняття рішень у галузі інформаційної безпеки для підприємця є пріоритетним завданням. А наступним завданням є переведення поінформованості на рівень практичних дій – усунути причину і наслідки порушення безпеки.

Інформаційна безпека і безпека економічна тісно взаємопов'язані і їх слід розглядати в комплексі, а не окремо кожну. Не можна забезпечити економічну безпеку підприємства, не вирішивши завдань із захисту каналів доставки інформації й інформаційного продукту. З огляду на інертність мислення в керівництва не завжди вистачає волі на прийняття рішень, які відразу не дають ефективного прибутку, тому завдання щодо забезпечення інформаційно-економічної безпеки вирішуються за остаточним принципом.

Центральним завданням статті є висвітлення стану справ із захистом відкритих мереж і мотивація керівництва підприємств щодо посиленого приділення уваги питанням захисту економічної безпеки.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Важливим фактором є час, необхідний для ідентифікації загрози для інформаційно-економічної безпеки та її подальшого усунення. Щодо фізичної загрози люди мають достатньо часу для вирішення цього завдання – від кількох хвилин до кількох тижнів. Інша справа в кіберпросторі – це секунди і мілісекунди. І порушник завжди перебуває в більш вигідному положенні ніж захисник системи. Порушник шукає одне слабке місце в системі, через яке і здійснює атаку, а захисник системи повинен контролювати, як правило, кілька сотень вразливостей своєї системи [1; 7; 8]. Звичайно, що він це робить не візуально, а на рівні застосування відповідних технологій. Із цього можна зробити висновок про те, що технології виявлення і знешкодження загроз повинні бути такими, щоб надійно утримувати під контролем вразливості системи й одночасно не дати порушнику ними скористатися. Кіберсередовище вимагає застосування сучасних технічних і організаційних контрзаходів, які б своєчасно й автоматично реагували як на наявні в системі вразливості, так і на загрози.

Потенціал можливих загроз для економічної безпеки ще достатньо не вивчений. І далеко не всі загрози на сьогодні є зрозумілими для працівників служби безпеки на підприємстві, тому адміністратори безпеки реагують лише на ті загрози, які їм зрозумілі. Очевидно, що загроз і ризиків значно більше. Чинні сьогодні традиційні системи захисту не дають повної картини про уразливість (слабкі місця) системи і забезпечують, за різними думками фахівців, захист від загроз не більше 30%. Брак вичерпної інформації про весь арсенал можливих загроз для економічної безпеки підприємства створює ілюзію захищеності.

Активність, професійна майстерність і технологічність порушників безпеки зростає. Вони починають діяти групами, скоординовано, з декількох географічно розподілених точок. Постійний розвиток інформаційних технологій викликає цілу низку нових проблем, а тому діагностика потенційних загроз повинна бути більш досконалою, системною, всеосяжною [12, с. 76–78].

Є таке поняття як «політика безпеки». Це своєрідна технологічна карта для дій адміністраторів безпеки від виявлення загрози до її знищення. Скорочення часу між цими позиціями – від виявлення до знищення – ось ключ до ефективної системи захисту інформаційних ресурсів і, як наслідок, економічної безпеки підприємства.

Важливе значення для підтримання на належному рівні економічної безпеки підприємства має наявність добре тренованого персоналу, який: чітко дотримується технологічної дисципліни, своєчасно і системно застосовує процедури і технічні засоби захисту, проводить аналіз потенційних атак і зловживань [3, с. 55–61; 10, с. 83].

Безперервний розвиток мережевих технологій через брак постійно проведеного аналізу їх безпеки призводить до того, що з плином часу захищеність мережі падає, тому що з'являються нові невраховані загрози і вразливості системи, протиставити яким нічого. Підхід до створення надійної системи мережевої безпеки повинен будуватися на основі політики безпеки, традиційних засобів захисту, результатів аналізу загроз і реалізації контрзаходів. Це

зробить систему захисту економічної безпеки підприємства більш ефективною.

За логікою процесу побудови системи захисту, вона повинна починатися з оцінки потенційної загрози, як фундаменту всієї подальшої роботи. Тобто спочатку треба виявити загрозу, потім оцінити рівень її небезпеки, визначитися з її спрямуванням щодо наявних вразливостей системи і прийняти правильне рішення, яке буде адаптуватися до нових умов мережевого оточення. Водночас треба робити поправку на те, що технології постійно розвиваються, практично щомісяця з'являються нові програмні забезпечення. Злочинці стають більш досвідченими, обізнаними й озброєними щодо атак на систему економічної безпеки підприємств, установ, банків, компаній. Збільшуються потреби в додатковому використанні Інтернет-ресурсу серед підприємців, а його нестача для забезпечення захисту призводить до того, що організаціям потрібно інший підхід до забезпечення інформаційної безпеки, щоб дозволяв іти в ногу з постійними технологічними змінами [10, с. 77].

Для того, щоб знизити рівень загроз для економічної безпеки, необхідно розробити такий механізм реагування, який був би високочутливим до змін і працював у реальному режимі часу. Фахівці в галузі інформаційних технологій називають такий механізм адаптивною безпекою (Adaptive Network Security, ANS). Адаптивна безпека (ANS) – це саме той підхід, який дозволяє контролювати, виявляти і реагувати в реальному режимі часу на ризики безпеки, використовуючи правильно спроектовані і добре керовані процеси і засоби.

Компанія "Yankee Group" (має дослідницьке спрямування у своїй діяльності) у червні 1998 р. опублікувала звіт, у якому ANS описано як процес, який містить: *технологію аналізу захищеності або пошуку вразливостей; технологію виявлення атак; адаптивний* компонент, який містить у собі і розширює дві перші технології; *керуючий* компонент.

Аналіз захищеності є технологічною процедурою, яка здійснює пошук вразливих місць у мережі. Структурно-організаційно мережа складається із безпосередньо комп'ютерів, з'єднань і вузлів, робочих станцій, додатків і баз даних, які є найбільш вразливими і потребують захисту, а це неможливо здійснити ефективно, якщо не проведено аналіз. І якщо система, що реалізує цю технологію, містить адаптивний компонент, то усунення виявлених уразливостей буде здійснюватися автоматично. До найбільш типових проблем, які виявляються в результаті аналізу, належать «дірки» в системах, програми типу «троянський кінь», брак необхідних оновлень, слабкі паролі, неправильне налаштування міжмережевих екранів, Web-серверів і баз даних тощо [10, с. 74]. Це те, що керівник, який по-справжньому дбає про економічну безпеку свого підприємства, повинен постійно тримати в полі зору. Наприклад, періодичну зміну паролів.

Технології аналізу захищеності здійснюють діагностику і на основі отриманих результатів реалізують заходи щодо мережевої безпеки раніше, ніж здійсниться спроба її порушення ззовні або зсередини організації. Виявлення атак на систему безпеки має технологічну основу і в межах цієї статті розглядатися не буде. Але, щоб було зрозуміло, прикладом адаптивного компоненту є механізм оновлення баз даних антивірусних програм для виявлення нових вірусів.

Використання моделі адаптивної безпеки мережі дає можливість контролювати практично всі загрози і своєчасно реагувати на них високоефективним способом, що дозволяє не тільки усунути уразливості, які можуть привести до реалізації загрози, а й проаналізувати умови, що призводять до появи вразливостей. Ця модель також дозволяє зменшити зловживання в мережі, підвищити обізнаність користувачів, адміністраторів і керівництво компанії про події безпеки в мережі.

Технології, за якими будуються системи виявлення атак, традиційно (не регламентовано документами) прийнято умовно ділити на дві категорії: виявлення аномальної поведінки і виявлення зловживань. Практично ж, виявлення атак відбувається на рівні мережі і на рівні хоста (комп'ютера). На рівні мережі аналізується трафік, а на рівні хоста – операційні системи і програми. Такі підходи і така класифікація відображають ключові можливості, що відрізняють одну систему виявлення атак від іншої. Наскільки необхідними є такі знання, щодо систем захисту безпеки, для керівника підприємства, компанії питання неоднозначне. Але на цьому етапі розвитку кіберзлочинності і вже в найближчому майбутньому без таких знань, а може й значно глибших, не можна буде побудувати успішний бізнес [10, с. 72].

Кожний елемент плану, кожна бізнес-позиція буде формуватися на засадах системи захисту інформаційно-економічної безпеки. Навіть поверхневий аналіз технологій управління бізнесом свідчить про зростання кількості систем на основі інформаційних і телекомунікаційних технологій.

Висновки. Отже, адаптивний підхід щодо побудови системи захисту економічної безпеки підприємства, найімовірніше, на найближчу перспективу буде визначальним. Він є більш життєздатним, оскільки адаптивна система захисту чутливо реагує на зміни основних технологічних параметрів у кіберпросторі. Яскравим прикладом цьому є антивірусні системи виявлення атак, що працюють за цією технологією. Алгоритм, на основі якого працює адаптивна система захисту економічної безпеки підприємства, передбачає таку послідовність операцій: аналіз потенційних загроз і виявлення серед них таких, що реально загрожують підприємству (аудит); ретельне вивчення ситуації із загрозами щодо динаміки розвитку рівня їх небезпеки; формування плану заходів відповідно до політики безпеки підприємства та його реалізації.

Щодо наукової перспективи розгляду зазначеної проблеми слід вказати, що вона має кілька аспектів. Наприклад, методологія формування критеріальної основи щодо політики економічної безпеки підприємства та дослідження чинників, що впливають на формування критеріїв.

Іншим аспектом наукового інтересу до проблеми є механізм взаємообумовленості інформаційної та економічної безпеки. Це зумовлено тим, що комп'ютерні мережі не залежать від бізнесу і конкретних компаній завдяки відкритості технічних стандартів Інтернету.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Вишнівський В. Новий підхід до організації освітньої діяльності по підготовці ІТ-спеціалістів як основи забезпечення економічного росту держави / В. Вишнівський // Матеріали міжнародної науково-практичної конференції «Сучасні інформаційно-телекомунікаційні технології» (17–20 листопада 2015 р.). – К. : ДУТ. – 2015. – Т. 5. – С. 55–61.
2. Шевченко В. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави / В. Шевченко // Матеріали міжнародної науково-практичної конференції «Сучасні інформаційно-телекомунікаційні технології» (17–20 листопада 2015 р.). – К. : ДУТ. – 2015. – Т. 5. – С. 76–78.

3. Петрик В., Штоквиш О., Галамба М. Спеціальні інформаційні операції в економічному протиборстві / В. Петрик // Юридичний журнал. – 2007. – № 3 (www.justinian.com.ua).
4. Гудзь О. Розвиток ІТ-інновацій в Україні : перспективи та ризики / О. Гудзь // Матеріали регіонального семінару Міжнародного Союзу електрозв'язку «Тенденции развития конвергентных сетей : решения пост-NGN, 4G и 5G» (17–18 листопада 2016 р.). – К. : ДУТ. – 2016. – Т. 5. – С. 195–197.
5. Бордман Б. Засоби системного моніторингу рівня підприємства // Мережі і системи зв'язку. 1999. – № 5.
6. Лукацький О. Засоби аналізу захищеності – зробіть правильний вибір // Світ Internet. 1999. – № 4.
7. Лукацький О. Системи виявлення атак // Банківські технології. 1999. – № 2.
8. Толубко В. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : Монографія. – К. : НАОУ, 2003. – С. 27–30.
9. Арамов В., Клименко С. Базові технології комп'ютерних мереж : навчальний посібник. – К. : ун-т ім. Б. Грінченка, 2014. – 264 с.
10. Електронні платіжні системи : навчальний посібник / Ю. Тараненко, Н. Буличева, О. Кузьменко та ін. ; [За заг. ред. доцента Ю. Тараненка] – К. : ТОВ «Три К», 2013. – 229 с.
11. Гранатуров В. Управління послугами зв'язку: навчальний посібник / В. Гранатуров, І. Литовлченко. – К. : Освіта України, 2010. – 254 с.
12. Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України : матеріали парламентських слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та зв'язку ; ред. кол. : О. Данченко (голова), Г. Андрощук, О. Старинець, О. Баранов [та ін.]. – К. : Парлам. вид-во, 2016. – 256 с.