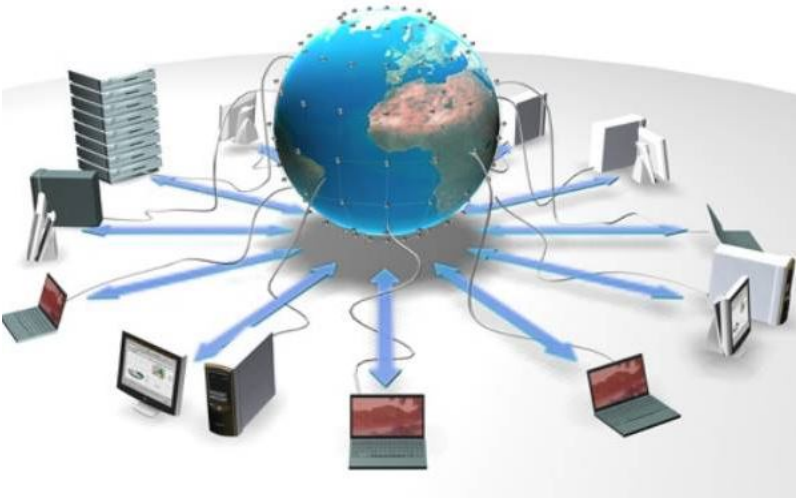
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ І УПРАВЛІННІ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 1



Одеса
2019

БЕЗПЕКА ЕЛЕКТРОННОГО БІЗНЕСУ

Бистра К. І.[1], **Орлик О. В.**[2]

1 – студентка 1 курсу 10 гр., факультет міжнародної економіки,
2 – канд. екон. наук, доцент, кафедра економічної кібернетики та інформаційних технологій
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Бистра К. І., Орлик О. В. ***Безпека електронного бізнесу.*** *У статті розглянуті питання безпеки електронного бізнесу. Проаналізовано найбільш вагомі кіберінциденти на підприємствах. Висвітлено недоліки розрахунків за допомогою Інтернет-банкінгу. Охарактеризовано основні напрямки захисту електронного бізнесу. Розглянуто засоби захисту електронного бізнесу від зовнішніх загроз.*

Ключові слова: *електронний бізнес, захист, Інтернет-банкінг, загрози, засоби захисту.*

Быстрая К. И., Орлик О. В. ***Безопасность электронного бизнеса.*** *В статье рассмотрены вопросы безопасности электронного бизнеса. Проанализированы наиболее значимые киберинциденты на предприятиях. Освещены недостатки расчетов с помощью Интернет-банкинга. Охарактеризованы основные направления защиты электронного бизнеса. Рассмотрены средства защиты электронного бизнеса от внешних угроз.*

Ключевые слова: *электронный бизнес, защита, Интернет-банкинг, угрозы, средства защиты.*

Bystra K. I., Orlyk O. V. ***E-business security.*** *The article discusses the security of electronic business. Analyzed the most significant cyber incidents in enterprises. Highlights the shortcomings of calculations using Internet banking. The main directions of e-business protection are characterized. Considered means of protecting e-business from external threats.*

Keywords: *e-business, security, Internet banking, threats, means of protection.*

ПОСИЛАННЯ НА РЕСУРС

Бистра К. І., Орлик О. В. *Безпека електронного бізнесу* // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2019. Вип. 1. С. 108–112.

Постановка проблеми у загальному вигляді. В умовах сучасного ринку товарів та послуг підприємці використовують безліч різних видів ведення бізнесу. Одним з найпопулярніших видів є електронний бізнес. Такий вид діяльності має великі переваги: збільшення ринку збуту, цілодобовий доступ, відсутність потреби в організації місця проведення торгівлі, проведення різного роду операцій незважаючи на відстань, розповсюдження інформації, зв'язок з клієнтом та ін. Але такі сучасні технології створюють сприятливі умови для злочинної діяльності у мережі Інтернет.

Аналіз досліджень і публікацій останніх років. Темою безпеки електронного бізнесу займається багато вітчизняних та зарубіжних науковців, оскільки наразі це актуальна тема серед дослідників сфери інформаційних технологій. Безпеку електронного бізнесу розглядають Ю. Бондарчук, С. Савін, Н. Сулік, Н. Васильєва, А. Гінкул, В. Кавура та ін

Виділення невирішених раніше частин загальної проблеми. Незважаючи на наукові дослідження і роботи з даної тематики, проблеми захисту електронного бізнесу сьогодні потребують подальшого вивчення. Це пов'язано є занадто швидкими темпами розвитку технологій, що відкривають все більше прогалин у захисті електронного бізнесу. З цієї причини необхідним є застосування перевірених та нових засобів для вирішення питань злочинності у мережі Інтернет.

Мета статті. Метою статті є розкриття проблеми безпеки електронного бізнесу, визначення основних напрямків та засобів організації та підтримки безпеки, які дозволяють забезпечити стабільний рівень захисту.

Виклад основного матеріалу дослідження. ***Електронний бізнес*** – це ділова діяльність в мережі Інтернет, яка базується на інформаційних технологіях. Такий бізнес з'явився внаслідок активного розвитку служб Інтернету. Для електронного бізнесу одним з найважливіших факторів діяльності є безпека, яка забезпечує стабільну роботу підприємства.

Згідно з даними дослідження «Лабораторії Касперського» за участю понад 350 представників індустріальних організацій по всьому світу кожна друга промислова компанія в світі у 2017 році пережила від одного до п'яти кіберінцидентів, які зачепили критично важливі інфраструктури або автоматизовані системи управління технологічними процесами на цих підприємствах [5].

Найбільше на сьогоднішній день компанії побоюються можливості зараження шкідливим програмним забезпеченням. І це не дарма, про що свідчать дані, наведені на рис. 1. 53% постраждалих від кіберінцидентів підприємств підтвердили випадки зіткнення з різними зловредами. 36% (близько третини компаній), піддавалися таргетованим (цільовим) атакам. Таким чином, шкідливі програми і добре сплановані цілеспрямовані операції стали домінуючими загрозами для промислових і критично важливих інфраструктур.

Компанії часто недооцінюють внутрішні загрози, побоюючись ризиків ззовні. Так, 44% компаній вважають, що їх кібербезпеці з великою

часткою ймовірності будуть загрожувати будь-які треті особи, 33% компаній вважають, що найбільшу небезпеку для них представляють програми-вимагачі. Однак частіше кіберінциденти в промислових мережах трапляються через помилки і ненавмисні дії персоналу – саме цей фактор погрожував майже третині компаній (29%).

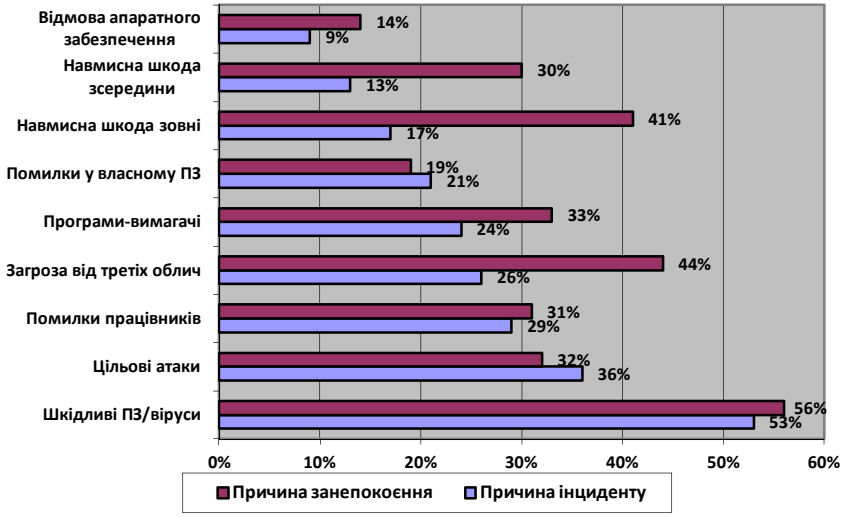


Рис.1. Види кіберінцидентів та їх зустрічальність [5]

Від безпеки залежить прибуток електронного бізнесу, оскільки розрахунки здійснюються через Інтернет-банкінг, який надає клієнту можливість керувати власними коштами через Інтернет.

Небезпекою такого виду розрахунків є ризик проникнення злодія в систему E-money. Завдяки сучасним технологіям можливо не лише пограбувати власника електронного гаманця, а й сфальсифікувати Інтернет-кошти [2, с.120].

Основні недоліки Інтернет-банкінгу: криптографічний захист, який не має тривалого досвіду успішного користування; можливість вистежування даних платників; недостатня зрілість технологій захисту [4].

Основні види шахрайських дій: розрахунок за реквізитами вкрадених кредиток, організація шахрайських Інтернет-магазинів, злам баз даних [1, с.92].

В цілому організацію безпеки електронного бізнесу можна розглядати за трьома напрямками захисту: організаційному, техніко-технологічному, нормативно-правовому [7].

Організаційний захист – регламентація виробничої діяльності та взаємовідносин суб'єктів господарювання й партнерів на основі нормативно-правової бази, що виключає або ускладнює неправомірний доступ до конфіденціальної інформації, появу внутрішніх та зовнішніх загроз та знижує ризик завдання збитків.

Організаційний захист відбувається на основі створення внутрішньої політики захисту компанії. До організаційного захисту належать такі дії:

– перевірка програмного забезпечення на предмет хакінгу;

– ретельне вивчення кожної кібератаки, незалежно від того, наскільки успішно вона завершилася;

– створення послідовності чітких дій у випадку спотворення чи видалення інформації;

– введення загальної культури дотримання безпеки в компанії;

– розробка правил з дотримання безпеки для працівників;

– щорічні тренінги для персоналу з питань безпеки та кіберзлочинності.

Техніко-технологічний захист – використання технічних та програмних засобів, що перешкоджають завданню збитків суб'єктам господарювання при здійсненні ними бізнес-операцій онлайн.

Техніко-технологічний захист допомагає виключити будь-яку можливість несанкціонованого доступу до різного роду даних та інформації. Для такого виду захисту використовують такі дії:

– надання мінімального обсягу прав для роботи з системою;

– регулярна зміна паролів та їх підтримка;

– своєчасна зміна доступу для працівників при кадрових змінах або негайне знищення доступу при звільненні працівника.

Нормативно-правовий захист – заходи, процедури, закони, правові акти та правила, що надають захист інформації на правовій базі.

Нормативно-правовий захист забезпечує наявність відповідних нормативно-правових елементів: таких як патенти, авторські права, у т. ч. на інтелектуальну власність, ліцензії, закони, положення, накази, стандарти та інше, що надає правові гарантії безпеки електронного бізнесу.

Необхідною умовою підтримки безпеки електронного бізнесу є забезпечення захисту інформації від зовнішнього впливу. Для цього існують різні засоби, які виступають свого роду фільтрами, що допомагають виявити спроби атак на ранніх етапах і по можливості не допустити зловмисника в систему через зовнішні мережі. Засоби захисту від зовнішнього втручання представлені в табл. 1.

Таблиця 1

Засоби захисту від зовнішнього втручання (розроблено на основі [6])

Засоби захисту	Характеристика
1	2
Маршрутизатори	Керують трафіком мережі та контролюють вхідний і вихідний трафіки приєднаних до нього сегментів мережі.
Системи відстеження вторгнень (Intrusion Detection Systems)	Виявляють навмисні атаки та неправильне використання системних ресурсів користувачами.
Шлюзи додатків	За допомогою них адміністратор мережі реалізує політику захисту, якою керуються маршрутизатори, що здійснюють пакетну фільтрацію.

Продовження таблиці 1

1	2
Брандмауери	Ізолюють приватні мережі від мереж загального користування, захищаючи систему шляхом певного контролю типів запитів.
Засоби оцінки захищеності	Програми (спеціальні сканери, ін.), які регулярно сканують мережу та тестують на предмет наявності проблем та ефективності захисту.

Висновки з даного дослідження. Електронний бізнес є перспективним напрямом розвитку підприємств, що за сприятливих умов може дійти високого рівня розвитку та позитивно вплинути на економіку підприємств і держави в цілому. Нехтування його безпекою може мати серйозну загрозу для підприємства і призвести до негативних наслідків у його діяльності. Разом із розвитком технологій розвивається і злочинність, тому слід постійно слідкувати за тенденціями покращення захисту свого підприємства.

ЛІТЕРАТУРА

1. Дробышева В. Г., Черноиванов А. П. Роль и место информационных технологий в системе экономической безопасности государства // Социально-экономические явления и процессы. 2011. № 3-4. С. 87–93.

2. Банковское дело : учеб. / Под ред. О. И. Лаврушина. М. : Финансы и статистика, 2004. 120 с.

3. Савин С. С. Анализ и оценка рисков.// Вестник Российской экономической академии имени Г. В. Плеханова. № 3. 2006. С. 96–104.

4. Шкарупелова А. С., Трунина В. Ф. Проблемы безопасности использования электронных денег // Тенденции развития экономической науки и менеджмента: материалы междун. заоч. науч.-практ. конференции. Новосибирск : Изд. «ЭКОР-книга», 2012. С. 26–30.

5. Киберпреступность в мире. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5 (дата звернення: 19.04.2019).

6. Безпека в електронного бізнесі. URL: http://fuck-hack.com/bezpeka-v-elektronnomu-biznesi/ (дата звернення: 19.04.2019).

7. Васильєва Н. Ф., Гінкул А. С., Кавура В. Л. Організація безпеки онлайнового електронного бізнесу. URL: https://cyberleninka.ru/article/n/organizatsiya-bezopasnosti-onlaynovogo-elektronnogo-biznesa (дата звернення: 21.04.2019).

8. Фінансово-економічна безпека підприємств та інформаційні технології забезпечення безпеки : монографія / О. В. Орлик, О. О. Кюне, О. Г. Єсіна, А. Ю. Вакула. Одеса : ФОП Гуляєва В.М., 2018. 140 с.

9. Орлик О. В. Інформаційні технології забезпечення безпеки електронного бізнесу // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конференції (Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 167–169.

10. Орлик О. В. Проблеми забезпечення інформаційної складової економічної безпеки сучасних підприємств // Кібербезпека в Україні: правові та організаційні питання : матеріали III Всеукр. наук.-практ. конференції (Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 79-81.