УДК 04.002+658.5

КІБЕРБЕЗПЕКА, ЯК ФАКТОР ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В АПВ

Левкін А. В., к.т.н., доц., e-mail: Artur.lav@3g.ua
Котко Я. М., к.е.н., ст. викл., e-mail: kotkoyana@ukr.net
Державний біотехнологічний університет, Україна
Левкіна Р. В., д.е.н., проф., e-mail: Levkina@3g.ua
Національний університет «Одеська політехніка»

Актуальність дослідження. Поява нових ІТ-технологій останніми роками сприяло численним перевагам та виникненню низки проблем, зокрема, зросла інтенсивність кібератак на ІТ-системи підприємств, у тому числі, агропромислового виробництва, процеси збереження й передачі інформації у підприємницькій діяльності. Як відомо, комплексна система кібербезпеки підприємств АПВ включає в себе систему тактичного інформаційного захисту (діагностика та виявлення інформаційних загроз), систему забезпечення стратегічного пріоритету (інформаційно-організаційна політика та стратегії інформаційного захисту підприємства), що дозволяє гарантувати стабільне функціонування та розвиток. Головним завданням системи кібербезпеки залишається захист його комерційної та економічної інформації, що характеризує всі аспекти господарської діяльності. Проте для досягнення вказаної мети потрібно розробити та запровадити нову політику кібербезпеки, яка відповідає сучасному стану розвитку інформаційних систем, має певний потенціал розвитку з огляду на виклики сучасної кібербезпеки та прагнення суб'єктів протистояти виникненню кіберзагрози, та необхідність виявлення й аналізу намірів нападу, слабких місць кібернетичної безпеки конкретного підприємства. Дослідженнями наукових проблем розробки системи кібербезпеки для підприємств АПВ, що пов’язані, зокрема, із удосконаленням механізму виявлення кібератак та створення дієвої моніторингової системи забезпечення кібербезпеки, займалися такі закордоні вчені як: A. Bessi, L. Bilge, R. Breu, J. S. Brownstein, N. Cuppens-Boulahia, F. Cuppens, P. Chakraborty, M. Dell’Amico, R.J. Ellison, E. Ferrara, C.H. Ong, E. Pontes. Серед вітчизняних вчених необхідно назвати таких як: В.Б.Авер’янова, В.В.Собчук, [2], К.Ю.Галинський, О.Г. Корченко, О.Є.Користіна, Р.С.Мельника, А.І.Марущака, А.В. Міщенко, О.В.Орлова, О.В.Олійник, Є.В.Петров, В.А.Савченко, О.І.Харитонову, Ю.Є.Хохлачов, Г.В. Шуклін та ін. В умовах сучасних ринкових трансформацій ІТ-технології набувають нового значення у контексті зростання актуальності питань щодо формування і реалізації передумов ефективного функціонування та пріоритетного розвитку підприємств АПВ. Такі технології повинні забезпечувати функціонування системи кібербезпеки підприємства, основним завданням якої є захист підприємницької інфраструктури, а саме: перевірка постачальників ресурсів, захист від поширення недостовірної й вірусної інформації, мінімізація кіберзагроз та кібератак. Зі зростанням вірогідності кіберзагроз у сфері АПВ зростає потреба у розробці тактичних дій і формування комплексної стратегії кібербезпеки підприємства, що повинні враховувати наступні складові: залежність інформаційно-технічної інфраструктури підприємства від іноземних технологій; залежність системи кіберзахисту інформаційно-телекомунікаційних систем від рівня вразливості програмно-апаратного обладнання, а саме, виявлення причин витоку важливої інформації; державна політика в галузі забезпечення кібербезпеки; механізм контролю та відповідальності учасників мережі Інтернет у сфері інформаційно-комунікаційних технологій та інше [3].

Основні матеріали дослідження. Наразі підприємницька діяльність в АПВ потребує ефективної системи кіберзахисту, яка використовується при взаємодії із потенційними споживачами, партнерами та при автоматизації внутрішніх процесів діяльності. Адже відомо, що результати порушення рівня кібербезпеки не лише призводять до величезних збитків, а й можуть бути критичними. На практиці існує декілька підходів забезпечення достатнього рівня кібербезпеки: *традиційнийпідхід* – базується на обмеженні використання брандмауера, антивірусного пакету й засобів шифрування при захисті систем даних, пристроїв, технологій підприємства від кібератак; *інноваційно-комплексний підхід* –

базується на використанні сучасних технологій, формують інтегровану платформу кіберзахисту і забезпечують безпеку кінцевих точок (комп'ютери, віртуальні діски, вбудовані й мобільні пристрої та сервери, пристрої Інтернету речей, камери, холодильники, системи освітлення, пристрої гучного зв'язку, термостати тощо), безпеку електронної пошти, захист комерційної інформації та особистих даних. Таким чином відбувається найбільш повний і ефективний рівень забезпечення активів підприємства [4].У публікаціях описано декілька способів забезпечення кібербезпеки у напрямку запобігання ненавмисним втратам, пошкодження чи несанкціонованого доступу до конфіденційної інформації підприємницької діяльності. Таким є спосіб, що дозволяє безпечне з'єднання: публічні точки доступу до Wi-Fi, smart-пристрій до робочого ноутбука, модем або точка доступу. У іншому випадку враховується можливість постійного оновлення програмного забезпечення та операційних систем (встановлення останньої версії програми, оновлення та форматування персональних пристроїв, операційної системи, програм та іншого програмного забезпечення), що передбачає зміни пароля, акаунту, персональних бездротових мереж та пристроїв. Спосіб економічно-інвестиційного забезпечення передбачає зв'язок нематеріальних активів із хмарним середовищем, хмарне резервне копіювання програмного забезпечення, що постійно й автоматично копіює усі файли і данні користувачів, сканує робочий процес (використовується відновлення файлів як елемент захисту цифрових активів, а резервне копіювання як засобом для цього). Спосіб сканування даних антивірусними програмами та шифрування використовується при передачі конфіденційної інформації, оскільки передбачає складний алгоритм та ключі шифрування [5]. Разом з тим системного дослідження вимагають питання ефективного попередження кібератак саме для підприємств АПВ і їх підприємницької діяльності: комунікаційні бізнес-процеси, де захист критичної інформації у електронній документації є найбільш складним: корпоративна документація, реквізити фінансових рахунків, податкова звітність (більшість інструментів інформаційного захисту є безкоштовними завдяки веб-браузерам SLUCK, Google Hangout, Skype і забезпечують конфіденційність програм); процеси соціальної комунікації, де найвищий рівень інформаційно-технічних ризиків і одночасний вплив на репутаційно-іміджеву систему підприємництва; фінансово-виробничі процеси (неправильна інтерпретація фінансової звітності й реалізація фінансової політики формує ризики невідповідності стратегічних пріоритетів) [6, 7].

Висновок. Висока ефективність реалізації ключових процесів підприємницької діяльності АПВ значною мірою залежить від використання сучасних високонадійних антивірусних та інших програм, що дозволяють попередити кіберризики підприємництва у АПВ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Веселова Л. Ю. Методологічні засади пізнання кібернетичної безпеки. *Південноукраїнський правничий часопис*. 2019. № 4. Ч. 2. С. 162-165.

2. Галахов Є. М., Собчук В. В. Розвиток моделей кібератак у площині інформаційної безпеки підприємства. *Телекомунікаційні та інформаційні технології.* Київ, ДУТ. 2019. № 4 (65). С. 12 – 24.

3. Білявська Ю., Микитенко Н., Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. *Товари і ринки*. 2021. № 1. С. 34-46.

4. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток.* 2019. №11. http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf

5. Гребенюк М. Деякі питання організаційно-правового забезпечення кібербезпеки : огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право.* 2019. №2. С. 203-207.

6. Дейнега О. В. Інформаційна безпека підприємств в умовах глобалізації 4.0. *Економіка та суспільство*. 2019. № 20. С. 199-208.

7.Levkin, A., Levkina, R., Petrenko A., Chaliy I. Economic Security as a Result of Modern Biotechnology Implementation. *Problems of Infocommunications Science and Technology (PIC S&T '2019): 2019 IEEE International ScientificPractical Conference* (October 8-11, 2019), Kyiv, 2019. Pp. 139-142.