Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України від 11.07.2019 № 975)
www.economy.nayka.com.ua | № 6, 2021 | 24.06.2021 р.

DOI: 10.32702/2307-2105-2021.6.80

УДК 659.2

В. В. Мельник,
к. е. н., доцент кафедри економіки та фінансів підприємства,
Київський національний торговельно-економічний університет
ORCID ID: 0000-0001-5512-536X
Т. В. Жук,
к. е. н., старший викладач кафедри економіки та фінансів підприємства,
Київський національний торговельно-економічний університет
ORCID ID: 0000-0001-5866-8837

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЯК СКЛАДОВА ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

V. Melnik
PhD in Economics, Associate Professor of the Department of Economics and Business Finance,
Kyiv National University of Trade and Economics
T. Zhuk
PhD in Economics, Senior Lecturer of the Department of Economics and Business Finance,
Kyiv National University of Trade and Economics

INFORMATION SUPPORT AS COMPONENTS OF FINANCIAL SECURITY OF THE ENTERPRISE

У статті досліджено інформаційне забезпечення підприємства. Розглянуто заходи щодо запобігання інформаційних ризиків в системі фінансового забезпечення підприємства. Запропоновано етапи інформаційного забезпечення фінансової безпеки підприємства. Розроблено схему інформаційного забезпечення фінансової безпеки підприємства. В основу схеми покладено система інформаційного забезпечення на адміністративному, процедурному та технічному рівнях. Адміністративний рівень забезпечує ефективність використання інформаційних ресурсів та попереджає загрози. Процедурний рівень забезпечує діагностику фінансових критеріїв та ідентифікацію джерел виникнення небезпек. Технічний рівень забезпечує захист фінансових інтересів і важливої інформації підприємства. Авторами запропоновано схему захисту інформаційної системи підприємства, як основи фінансового забезпечення підприємства. В основі схеми виокремлено: фізичний захист інформації, управління конфігурацією, супровід інформаційної системи, цілісність системи даних, управління доступом, реагування на порушення інформаційної системи, планування інформаційної безпеки.

The article studies the information support of the enterprise. The authors determined that most of the risks arise due to insufficient awareness of enterprises about changes that occur or may occur in the future in the macroeconomic environment. The category "information risks" was singled out, in particular two groups of such risks: external and internal production character, and also the ways of risk reduction and methods of their management at the enterprise were substantiated.

Considered measures to prevent information risks in the system of financial support of the enterprise. Stages of information support of the financial security of the enterprise are proposed. The scheme of information support of the financial security of the enterprise are developed. The scheme includes Information support systems at the administrative, procedural and technical levels. The administrative level ensures the efficient use of information resources and prevents threats. The procedural level provides diagnostics of financial criteria and identification of sources of danger. The technical level provides protection of the financial interests and important information of the enterprise. The authors analyze current trends in incidents and threats from criminals.
The largest number of incidents was in the financial and medical sectors of the economy. The peculiarities of incidents of different spheres of activity depending on their size are investigated. The authors traced the change in the sources of incidents in 2016-2020. Malware has taken last place. The use of "Trojan" had the same tendency. Began to increase the speed of use of "Misconfiguration" and "Misdelivery". The purpose of which is to obtain data through errors identified by the staff of the enterprise. "Phishing" and "Hacking" began to occupy leading positions. Identified changes in cyberattacks related to Covid-19. The authors offer a scheme for the protection of the information system of an enterprise as the basis for the financial support of an enterprise. The scheme is included: physical protection of information, configuration management, information system maintenance, data system integrity, access control, response to information system violations, information security planning.

Ключові слова: *інформаційне забезпечення; фінансова безпека; інформаційні ризики; інформаційна безпека; кібератака; кібербезпека.*

Keywords: *information security; financial security; information risks; information security; cyberattack; cybersecurity.*

Постановка проблеми. Сучасний стан розвитку економіки висуває певні вимоги до діяльності підприємницьких структур, що зумовлює необхідність формування системи, яка б акумулювала інформацію фінансового характеру, сприяючи покращенню результатів фінансової діяльності підприємств у кризових умовах функціонування економіки України.

Це не лише підвищує вимоги до фінансової інформації, а й зумовлює необхідність вирішення нових завдань у сфері інформаційного забезпечення, зокрема визначення інформаційних ризиків і шляхів їх зниження на підприємствах у контексті забезпечення їх фінансової безпеки.

Аналіз останніх публікацій та досліджень. Серед праць, присвячених окремим питанням оцінювання та забезпечення фінансової безпеки різних галузей економіки висвітлено у працях провідних вітчизняних вчених О.В. Ареф'євої, О.І. Барановського, І.О. Бланка, В.В. Бурцева, О.С Власюка, К.С. Горячевої, О.В. Гривківської, М.Ю. Дмітрієва, М.М. Єрмошенка, А.М. Єрмошенко, Т.І Єфименко, Ю.Г. Кіма, І.А. Ломачинської, Г.А. Пастернак-Таранушенко та закордонних науковців: Ф. Айала, М. Маззолі, С.Майерса, Л. Ллойд, Л. Руе, П. Трейнар, Р.Холта.

Завдання статті. Пошук нових підходів до запобігання інформаційних ризиків, визначення алгоритму дій щодо диверсифікації інформаційних ризиків на різних рівнях інформаційного забезпечення, розробка комплексу заходів щодо захисту інформаційної системи задля фінансової безпеки підприємства.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Підвищення ефективності фінансової діяльності підприємства на основі забезпечення повноти і достовірності фінансової інформації передбачає реалізацію заходів у напрямах адаптації управлінських структур у відповідності з міжнародними стандартами, зниження фінансових ризиків на основі забезпечення повноти і достовірності фінансової інформації.

Досліджуючи різні форми підприємницьких структур було визначено, що більша частина ризиків виникає внаслідок недостатньої інформованості підприємств стосовно змін, які відбуваються або можуть відбутись у перспективі в макроекономічному середовищі. Отже, виділимо категорію «інформаційні ризики», зокрема дві групи таких ризиків: зовнішнього та внутрішньовиробничого характеру, а також обґрунтуємо шляхи зниження ризиків і методи управління ними на підприємстві.

Ризики внутрішнього характеру підприємства, виникають в результаті порушення фінансової дисципліни, помилок в управлінні тощо. Цим ризикам на підприємстві можна запобігти шляхом реалізації наступних заходів (рис. 1).

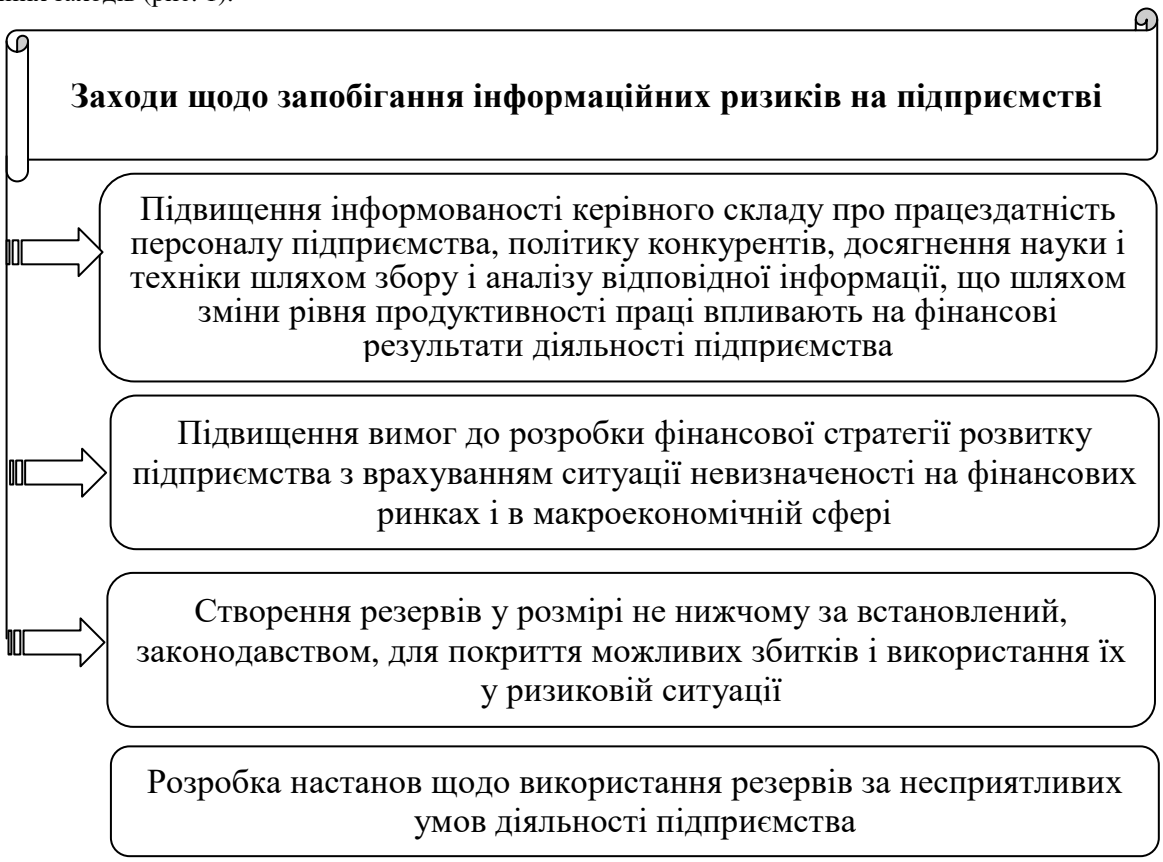

Рис. 1. Заходи щодо запобігання інформаційних ризиків на підприємстві
Джерело: систематизовано авторами на основі [1,2,3,5,6]

На підприємствах особливої актуальності набуває розробка заходів, спрямованих на зниження фінансових ризиків, які пов'язані з поверненням кредитів банківським установам, боргів – партнерам, працівникам підприємств, вкладникам тощо. Вирішення проблеми слід шукати в площині удосконалення юридичних основ, які мають захищати інтереси власників підприємства.

Після проведеного аналізу можемо запропонувати наступні етапи забезпечення інформаційної безпеки на підприємстві (рис. 2).

Рис. 2. Етапи інформаційного забезпечення фінансової безпеки підприємства
Джерело: систематизовано авторами на основі [5,6]

Інформаційне забезпечення фінансової безпеки підприємства – це процес формування та забезпечення інформаційної складової їх фінансової безпеки, що передбачає виконання сукупності функціональних обов'язків щодо інформаційно-аналітичного обслуговування діяльності підприємства [5].

Інформаційне забезпечення фінансової безпеки реалізується шляхом попереднього формування на підприємстві інформаційної системи як сукупності організаційних і технічних засобів для збереження та обробки інформації [7] та охоплює три рівні (рис. 3).

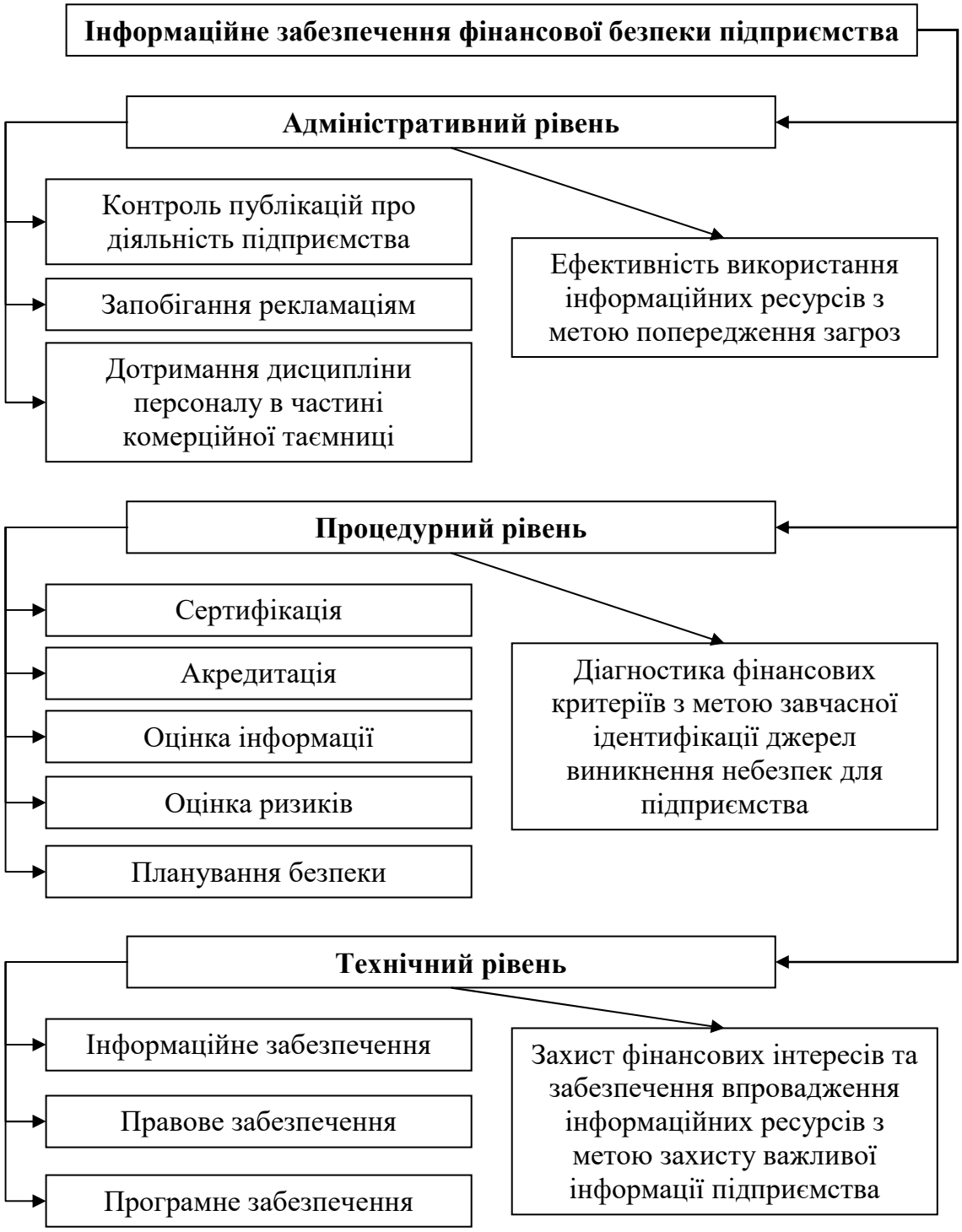

Рис. 3. Інформаційне забезпечення фінансової безпеки підприємства

У галузі сертифікації, акредитації й оцінки безпеки підприємства варто проводити:

- постійний моніторинг та оцінку регуляторів безпеки, що дозволяє сформувати довіру до ефективності їхнього застосування;

- розробка й реалізація на практиці плану дій по усуненню недоліків і зменшенню або усуненню уразливості інформаційної системи;

- авторизацію введення в експлуатацію інформаційної системи і встановлення з'єднань із іншими інформаційними системами.

- оцінка ризиків. Із заданою частотою або після появи відомостей про нові критичні для інформаційної системи уразливості необхідно сканувати уразливості в інформаційній системі.

- закупівля систем і сервісів. Необхідно включати в загальний пакет документів документацію від виготовлювача/постачальника (при наявності такої), що описує функціональні властивості регуляторів безпеки, задіяних в інформаційній системі, досить детальну для того, щоб уможливити аналіз і тестування регуляторів [2].

Досліджуючи інформаційне забезпечення фінансової безпеки будь-якого підприємства необхідно приділити увагу сучасним аспектам захисту інформації. Ковід-19 вплинув на діяльність підприємств всього світу. Більшість підприємств змушені були організувати віддалений режим роботи окремих працівників, підрозділів, всієї діяльності. Все це обумовило зміни умов роботи з внутрішньою інформацією підприємства. Непередбачуваність ситуацій, швидка зміна умов функціонування, недостатність технічної підтримки і оснащення підприємств призвели до успіху кібератак.

За даними компанії Positive Technologies кількість кіберінцидентів зросла на 51 % у 2020р. у порівнянні з 2019 р. Найбільша кількість інцидентів була зафіксована у фінансовій та медичній сферах. Хоча статистика в розрізі окремих країн може дещо відрізнятися. Компанія Verizon, яка дослідила кількість інцидентів та порушень не тільки за сферами діяльності, але і за розміром компанії, з'ясувала, що великі підприємства більше фокусується на дистанційній організації роботи з контрагентами, забезпечує доступ до своїх послуг за допомогою різних мобільних-додатків. Відповідно, великим підприємствам притаманна більша кількість ризиків, пов'язаних із захистом інформації, ніж малим. Крім того, основною метою кібератак все ще залишається фінансове питання. З огляду на це, чим більша компанія, тим на більший розмір фінансових вимог. Таким чином, за дослідженнями Verizon більша кількість кібератак була притаманна великим підприємствам таких сфер, як: виробництво, фінанси, роздрібна, оптова торгівля, транспорт; малим підприємствам у сферах: освіта, медицина, інформація, розваги. Кібератаки спрямовані на діяльність малих підприємств більшою мірою пов'язані з низьким рівнем безпеки захисту інформації. На основі досліджень Positive Technologies, Verizon, Trend Micro, Європейського агентства по мережевій і інформаційній безпеки Євросоюзу всі сфери діяльності підприємств і суспільства зазнали суттєвих збитків від кіберзагроз, кількість яких перевищує 62,6 млрд.

За дослідженнями компанії Verizon мотивом більше 60% інцидентів залишається фінансовий аспект, близько 30% - другорядні мотиви, шпіонаж – близько 10% [9]. За даними Positive Technologies метою зловмисників більше 60% всіх інцидентів є отримання даних, близько 40% - фінансова вигода [8]. Підприємства, на які відбулися кібератаки, витрачають значну суму для викупу конфіденційної інформації, якщо метою був фінансовий аспект, але, крім того, їх очікує значний розмір витрат для відновлення і подальшого захисту внутрішньої інформації. Так, Garmin по виробництву навігаційних сервісів сплатила викуп 10 млн. доларів для отримання ключа шифрування і успішно відновила свої системи [4]. Національна служба охорони здоров'я Великобританії понесла збитки близько 100 млн. доларів у результаті кібератаки [4]. Щорічно збитки тільки від BEC-атак складають близько 26 млрд. доларів [4].

Для організації захисту інформаційного забезпечення підприємства необхідно дослідити сучасні загрози. Verizon, визначила джерела порушення інформаційної безпеки підприємства, які представлені на рис. 4.

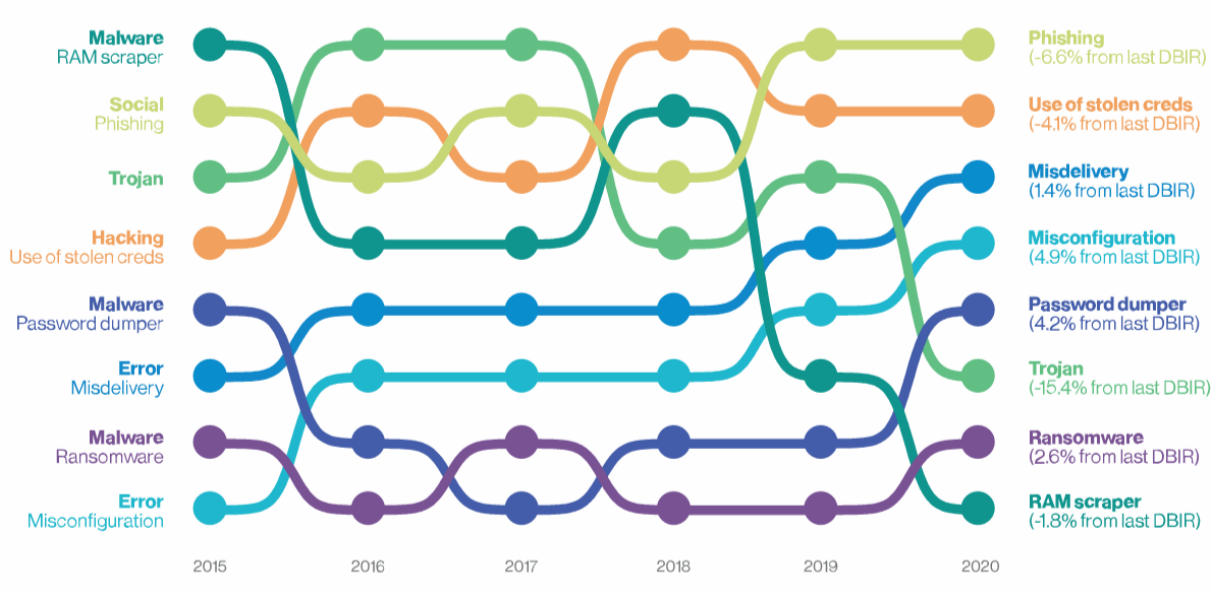

Рис. 4. Джерела інцидентів і порушень інформаційної безпеки підприємства [9]

За даними рисунка можна простежити, що шкідливе програмне забезпечення, метою якого є зчитування персональних даних, посідав перше місце у 2015 р., хоча у 2020 р. воно займало останнє місце. Таку саму тенденцію мало і застосування «Троян». У 2015-2020 рр. нарощують оберти використання «Misconfiguration» і «Misdelivery», які відносять до загального розділу «Помилка». Метою їх застосування є отримання даних через виявлені помилки персоналом підприємства. Останнім часом лідируючі позиції займає «Фішинг» і «Хакінг». За цими даними можна зробити висновок, що останнім часом зловмисники використовують джерела, які пов'язані з помилками трудового колективу підприємства. Крім того, а даними Positive Technologies найбільшу частку серед типів вкраденої інформації близько 27 % складає персональна

інформація [8]. А також основним вектором доставки шкідливого програмного забезпечення залишається електронна пошта (71%).

Ковід-19 став детермінантом для запуску нових видів і способів загроз інформаційної безпеки підприємства. У зв'язку з віддаленою роботою співробітникам підприємства змушені були одночасно вирішувати ряд задач. Такими задачами стало: забезпечення швидкого інтернет-зв'язку, відстеження використання персоналом робочого часу, організація зустрічей, розмежування особистих і робочих задач, організація захисту інформації не тільки в межах підприємства, але і на особистих пристроях персоналу тощо. Зловмисники швидко адаптувалися під зміни і стали використовувати розсилки на електронні пошти з інформацією про Ковід-19, які містили шкідливі файли і посилання. Найбільша частка від загальної кількості таких розсилок спостерігалася в Америці і складала 38,4 %, Німеччині – 14,6 %, Франції – 9,2% [8]. Атаки на домашні роутери збільшилася близько 20%. Частка bruteforce-атак на різні сервіси віддаленого доступу: RDP, SSH, FTP склала майже 90 % [8]. Активне використанні для онлайн-зустрічей стали: Zoom, Cisco Webex, Google Meet, Microsoft Skype та інші сервіси. У результаті чого з'явився «Зумбомбінг» та інші види атак, у результаті яких відбувалося підключення сторонніх осіб до нарад, приватних розмов тощо. Крім того, реєструвалися фішингові домени, ім'я яких було пов'язано із зазначеними вище сервісами, пропонуючи загружати дистрибутив, який містить шкідливий додаток.

Відомі компанії Microsoft, Zoom та інші намагаються протистояти кібератакам і постійно працюють над удосконаленням захисту інформації. Але і самим підприємствам необхідно розробляти систему захисту інформації від зовнішніх факторів. Враховуючи наведені вище дослідження сучасних загроз, керівникам підприємств необхідно подбати не тільки про технічну і кібербезпеку, але й про цифрову грамотність своїх працівників.

Враховуючи специфіку діяльності кожного підприємства необхідно розробляти систему заходів щодо захисту інформаційної системи підприємства. Інформаційне забезпечення фінансової безпеки підприємства вимагає реалізації наступних заходів щодо захисту роботи інформаційної системи (рис. 5).

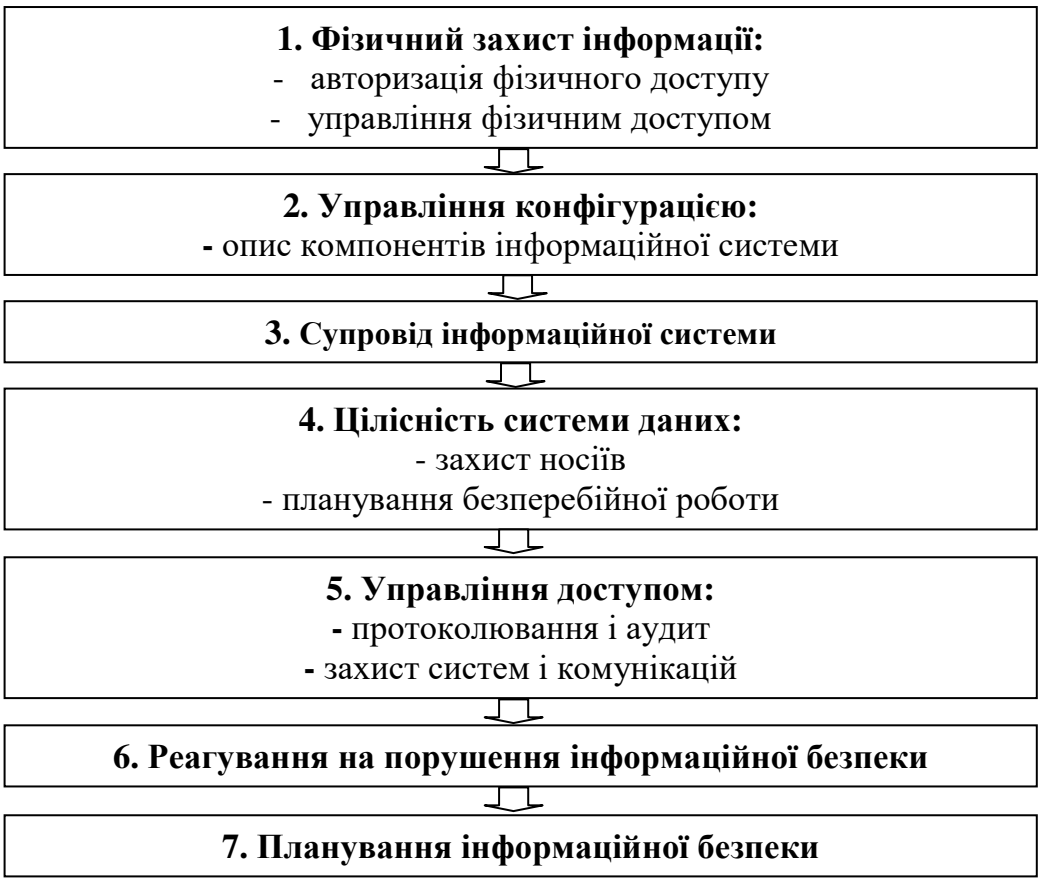

Рис. 5. Інфо-логічна схема захисту інформаційної системи підприємства, як передумови інформаційного забезпечення його фінансової безпеки

Джерело: систематизовано авторами на основі [1,2,3,5,6]

1. Фізичний захист інформації. Контроль фізичного доступу до устроїв відображення інформації з метою захисту останньої від перегляду неавторизованими особами.

З метою фізичного захисту підприємства повинні:

- надавати фізичний доступ до інформаційної системи, у робочі приміщення лише авторизованому персоналу;

- фізично захищати устаткування й підтримуючу інфраструктуру інформаційної системи;

- забезпечити належні технічні умови для функціонування інформаційної системи;

- захищати інформаційну систему від загроз з боку навколишнього середовища;

- забезпечити контроль умов, у яких функціонує інформаційна система;

- забезпечити управління доступом, надавши доступ до активів інформаційної системи лише авторизованим користувачам, процесам, що діють від імені цих користувачів, а також устроям для виконання дозволених користувачам транзакцій і функцій;

- розробити, поширювати, періодично переглядати й змінювати офіційну документовану політику фізичного захисту, у якій представлені мета, охоплення, ролі, обов'язки, підтримка керівництва, координація серед організаційних структур і відповідність чинному законодавству; формальні документовані процедури, що сприяють проведенню в життя політики й асоційованих регуляторів фізичного захисту;

- складати й підтримувати в актуальному стані списки співробітників, що мають доступ у приміщення, у яких розташовані компоненти інформаційної системи (крім приміщень, що офіційно вважаються загальнодоступними), випускаються відповідні посвідчення (бейджи, ідентифікаційні карти, інтелектуальні карти); відповідні посадові особи із заданою частотою переглядають і затверджують списки й посвідчення;

- контролювати точки фізичного доступу, у тому числі офіційно певні точки входу/виходу, у приміщення, у яких розташовані компоненти інформаційної системи (крім приміщень, що офіційно вважаються загальнодоступними);

- перевіряти надані співробітникам права, перш ніж дозволити їм доступ до використання даних інформаційної системи для обробки чи користування;

- установити й підтримувати базові конфігурації інформаційної системи;

- мати опис (карту) інформаційної системи, актуалізовану з урахуванням життєвого циклу, у яку входять апаратура, програмне забезпечення й документація.

2. Управління конфігурацією. У компанії розробляються, документуються й підтримуються актуальна базова конфігурація інформаційної системи, опис компонентів інформаційної системи і відповідні дані про їхніх власників:

- документуються й контролюються зміни в інформаційній системі; відповідні посадові особи санкціонують зміни інформаційної системи відповідно до прийнятої в організації політики й процедур;

- конфігурується інформаційна система так, щоб забезпечити лише необхідні можливості, і явно заборонити й/або обмежити використання певних функцій, портів, протоколів і/або сервісів.

3. Супровід інформаційної системи представлений:

- плануванням, здійсненням й документуванням повсякденного, профілактичного й регулярного супроводу компонентів інформаційної системи у відповідності зі специфікаціями виготовлювача або постачальника й/або організаційними вимогами;

- підтримкою списку осіб, авторизованих для здійснення супроводу інформаційної системи (зауважимо, що супровід інформаційної системи здійснює лише авторизований персонал);

- веденням реєстраційного журналу супроводу інформаційної системи, у якому фіксуються:

- дата й час обслуговування;

- прізвище й ім'я особи, яка проводила обслуговування;

- прізвище й ім'я супровідного, якщо це необхідно;

- опис зроблених дій по обслуговуванню інформаційної системи;

- список вилученого або переміщеного устаткування (з ідентифікаційними номерами).

4. Цілісність систем і даних досягається застосуванням засобів і методів моніторингу подій в інформаційній системі, виявлення атак і ідентифікація несанкціонованого використання інформаційної системи:

- захистом від спама;

- точністю, повнотою, вірогідністю і автентичністю даних;

- перевіркою даних на точність, повноту, вірогідність і автентичність;

- захистом носіїв: мітки носіїв, змінні носії даних і вихідні дані інформаційної системи забезпечуються зовнішніми мітками, що містять обмеження на поширення й обробку цих даних; задані типи носіїв або апаратних компонентів звільняються від міток, оскільки залишаються в межах контрольованої цілісності;

- плануванням безперебійної роботи. Підприємство координує розробку плану забезпечення безперебійної роботи зі структурами, відповідальними за родинні плани (наприклад, плани відновлення після аварій, реагування на порушення безпеки й т.п.);

- організацією навчання співробітників їхнім ролям і обов'язкам по забезпеченню безперебійної роботи інформаційної системи, а також із заданою частотою, але не рідше, ніж раз у рік, проводяться тренування для підтримки практичних навичок;

- телекомунікаційні послуги. Визначаються основне й запасне джерела телекомунікаційних послуг, що підтримують інформаційну систему.

Для уможливлення поновлення виконання інформаційною системою критично важливих виробничих функцій протягом заданого проміжку часу ініціюються необхідні угоди у випадках, якщо основне джерело телекомунікаційних послуг виявляється недоступним. Угоди про основні й запасні джерела телекомунікаційних послуг містять зобов'язання пріоритетного обслуговування відповідно до вимог організації до доступності.

5. Контроль і аудит. Інформаційна система забезпечує можливість включення в реєстраційні записи додаткової, більш детальної інформації для контролю дій, що ідентифікуються за типом, місцем або суб'єктом. Для забезпечення контролю та аудиту необхідно:

- створювати, захищати й підтримувати реєстраційні журнали, що дозволяють відслідковувати, аналізувати, розслідувати й готовити звіти про незаконну, несанкціоновану або неналежну активність;
- забезпечувати прозорість дій в інформаційній системі із точністю до користувача (підзвітність користувачів);
- захист систем і комунікацій: поділ додатків. Інформаційна система розділяє користувальницьку функціональність (включаючи сервіси користувальницького інтерфейсу) від функціональності управління інформаційною системою;
- захист систем і комунікацій: захист меж. Доцільно фізично розміщати загальнодоступні компоненти інформаційної системи (наприклад, загальнодоступні web-сервери) в окремих підмережах з окремими фізичними мережними інтерфейсами, запобігти публічному доступу у внутрішню мережу, за винятком належним чином контрольованого доступу.

З метою планування безперебійної роботи в компанії варто встановити, підтримувати й ефективно реалізувати плани реагування на аварійні ситуації, резервного копіювання, відновлення після аварій, щоб забезпечити доступність критичних інформаційних ресурсів і безперервність функціонування в аварійних ситуаціях.

6. Реагування на порушення інформаційної безпеки: реагування.

На підприємствах формуються структури для реагування на порушення інформаційної безпеки (група реагування), включаючи підготовку, виявлення й аналіз, локалізацію, ліквідацію впливу й відновлення після порушень.

За умови порушення інформаційного забезпечення фінансової безпеки підприємства доцільним є реагування наступного порядку:

- створення діючої структури шляхом запровадження підготовчих курсів та проведення інших заходів, зокрема виявлення, аналіз і локалізація порушень, відновлення після інцидентів і обслуговування користувачів;
- забезпечення відстежування, документування й повідомлення про інциденти відповідним посадовим особам організації й уповноваженим органам;
- навчання співробітників та моніторинг відповідності посад, які вони обіймають, їхнім вмінням та навикам, пов'язаним з реагуванням на порушення безпеки інформаційної системи, і із заданою частотою, але не рідше, ніж раз у рік, проведення тренувань для підтримки практичних навичок;
- підтримання процесу реагування на порушення інформаційної безпеки із застосуванням автоматичних механізмів;
- відстежування й документування порушення інформаційної безпеки.

7. Планування безпеки. Забезпечення належного планування й координації діяльності, пов'язаної з безпекою й інформаційною системою, з метою мінімізації негативного впливу на роботу й активи організації (у тому числі на її місію, функції, імідж і репутацію) [1,2].

Висновки і пропозиції. Проведені дослідження теоретичного та аналітичного характеру дозволяють зробити висновок, що інформаційне забезпечення є невід'ємною частиною фінансової безпеки підприємства. Сьогоднішні умови функціонування підприємств різних сфер діяльності обумовлюють необхідність розробки актуальної інформаційної системи, яка дозволить забезпечити фінансову безпеку підприємства. Основною перешкодою у побудові цілісної інформаційної системи підприємства є кібератаки зловмисників. Спираючись на результати досліджень виробників програмного забезпечення, Європейського агентства із забезпечення інформаційної безпеки Євросоюзу можна дійти висновків, що на підприємствах різних галузей відбулися порушення інформаційної безпеки, при чому, це притаманно, як великим, так і середнім підприємствам. Щорічне збільшення витрат підприємств на захист інформації, викуп бази даних у зловмисників та/або відновлення інформації, репутації викликає необхідність подальшого розвитку тематики, пов'язаною з інформаційним забезпеченням фінансової безпеки. З швидким розвитком технологій і розширенням спектру публічної інформації постає можливість проаналізувати кількість виявлених порушень в онлайн режимі в розрізі окремих країн. Можливості оброблювати великі масиви даних у питаннях ринку кіберстрахування, падіння котирування акцій у результаті кібератак, сум витрат на викуп вкраденої інформації (ключа шифрування та ін.) тощо дозволить провести більш точні розрахунки щодо понесених збитків. Прогнозні цифри щодо збільшення кількості кібератак та витрат, пов'язаних з ними, на 2021 р. підтверджують важливість подальшого розвитку теми.

Список літератури.

1. Віхорсв С. В. Як дізнатися – звідки напасти або звідки виходить загроза безпеці інформації / С.В. Віхорсв, Р.Ю. Кобцев // Захист інформації. Конфідент. – 2002. – № 2.
2. Генне О. В. Шпигунство в стільникових мережах / О.В. Генне // Захист інформації. Конфідент. – 2001. – №5.
3. Гонцяж Я. Свобода інформації та виконавча гілка влади: Правові норми. Інституції. Процедури. Порівняльний аналіз / Я. Гонцяж, Н. Гнидюк. – К.: Мілсніум, 2002. – 245 с.
4. Гончаров Е. Киберугрозы для промышленных предприятий в 2021 году / Е. Гончаров.

[Електронний ресурс]. – Режим доступу : https://securelist.ru/ics-threat-predictions-for-2021/99417/
5. Горячева К.С. Інформаційно-аналітичне забезпечення фінансової безпеки підприємства / К.С. Горячева // Актуальні проблеми економіки. – 2003. – № 9. – С. 43-49.
6. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення / М.М. Єрмошенко. – К. : Київ. нац. торг.- екон. ун-т, 2001. – 309 с.
7. Лазор Я. Поняття та види інформаційних систем / Я. О. Лазор // Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки. - 2016. - № 837. - С. 80-86.
8. Cybersecurity threatscape: 2020. [Електронний ресурс]. – Режим доступу : https://www.ptsecurity.com/ww-en/
9. Data Breach Investigations Report 2020. [Електронний ресурс]. – Режим доступу : https://www.verizon.com/business/resources/reports/dbir/

References.

1. Vikhorsv, S. V. (2002), “How to find out - where to attack or where the threat to information security comes from”, *Zakhyst informatsii. Konfident*, vol. 2, pp. 35–41.
2. Henne, O. V. (2001), “Espionage in cellular networks”, *Zakhyst informatsii. Konfident*, vol. 5, pp. 54–59.
3. Hontsiazh, Ya. and Hnydiuk, N. (2002), *Svoboda informatsii ta vykonavcha hilka vlady: Pravovi normy. Instytutsii. Protsedury. Porivnial'nyj analiz* [Freedom of information and the executive branch: Legal norms. Institutions. Procedures. Comparative analysis], Milsnium, Kyiv, Ukraine.
4. The official site of Kaspersky Company (2020), “Cyber threats to industrial enterprises in 2021”, available at: https://securelist.ru/ics-threat-predictions-for-2021/99417/ (Accessed 10 June 2021).
5. Horiacheva, K.S. (2003), “Information and analytical support of financial security of the enterprise”, *Aktual'ni problemy ekonomiky,* vol. 5, pp. 43–49.
6. Yermoshenko, M.M. (2001), *Finansova bezpeka derzhavy: natsional'ni interesy, real'ni zahrozy, stratehiia zabezpechennia* [Financial security of the state: national interests, real threats, security strategy], Kyiv. nats. torh.- ekon. un-t, Kyiv, Ukraine.
7. Lazor, Ya. (2016), “Concepts and types of information systems”, *Visnyk Natsional'noho universytetu «L'vivs'ka politekhnika». Seriia : Yurydychni nauky*, vol. 837, pp. 80–86.
8. The official site of company Positive Technologies (2021), “Cybersecurity threatscape: 2020”, available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (Accessed 10 June 2021).
9. The official site of company Verizon (2021), “Data Breach Investigations Report 2020”, available at: https://enterprise.verizon.com/resources/reports/dbir/2020/results-and-analysis/ (Accessed 10 June 2021).

Стаття надійшла до редакції 14.06.2021 р.