УДК 004:658.2 doi: 10.20998/2519-4461.2020.3.9

Н.Е. АВАНЕСОВА, О.С. МОРДОВЦЕВ, Т.В. КОЛОДЯЖНА

ФОРМУВАННЯ МЕХАНІЗМУ КОМПЛЕКСНОГО ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА УКРАЇНИ

У статті проведено дослідження теоретико-методичних та практичних аспектів комплексного забезпечення цифрової безпеки як основи для створення надійної системи інформаційної та економічної безпеки в рамках цифрової економіки на промисловому підприємстві України. Виявлено, що за допомогою цифрової економіки підвищується ефективність всіх промислових галузей за рахунок використання інформаційних технологій; якісно і кількісно збільшуються можливості здійснення через комп'ютер практично всіх господарчих операцій економіки. Визначено, що можливість внутрішнього та зовнішнього втручання в інформаційну систему промислового підприємства може негативно вплинути на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність тощо. Проведено аналіз основних досліджень концептуальних основ сутності категорій інформаційна безпека», «кібербезпека» та «цифрова безпека» на промислових підприємствах та надано узагальнене визначення категорії «цифрова безпека». Доведено, що цифрова безпека промислового підприємства полягає у формуванні принципів, методів та заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію та на основі цього сформовано механізм комплексного забезпечення цифрової безпеки промислового підприємства в умовах розвитку цифрової економіки України. В рамках розробленого механізму запропоновано побудувати ефективну стратегію впровадження та функціонування цифрової безпеки промислового безпеки на засадах визначених базових універсальних положень цієї стратегії. Запропоновано комплекс практичних заходів забезпечення реалізації стратегії цифрової безпеки промислового підприємства в режимі безперервного часу. Зроблено висновок, що для сучасного промислового підприємства вкрай важливо сформувати ефективну систему економічної та інформаційної безпеки, центральним місцем якої буде займати надійна цифрова безпека.

Ключові слова: економічна безпека; інформаційна безпека; цифрова безпека; цифрова економіка; кібербезпека

Н.Э. АВАНЕСОВА, А.С. МОРДОВЦЕВ Т.В. КОЛОДЯЖНАЯ

ФОРМИРОВАНИЕ МЕХАНИЗМА КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ УКРАИНЫ

В статье проведено исследование теоретико-методических и практических аспектов комплексного обеспечения цифровой безопасности как основы для создания надежной системы информационной и экономической безопасности в рамках цифровой экономики на промышленном предприятии Украины. Выявлено, что посредством цифровой экономики повышается эффективность всех промышленных отраслей за счет использования информационных технологий; качественно и количественно увеличиваются возможности осуществления через компьютер практически всех хозяйственных операций экономики. Определено, что возможность внутреннего и внешнего вмешательства в информационную систему промышленного предприятия может негативно повлиять на искажение таких параметров информации, как конфиденциальность, целостность, доступность, достоверность и тому подобное. Проведен анализ основных исследований концептуальных основ сущности категорий информационная безопасность», «кибербезопасность» и «цифровая безопасность» на промышленных предприятиях и дано обобщенное определение категории «цифровая безопасность». Доказано, что цифровая безопасность промышленного предприятия заключается в формировании принципов, методов и мероприятий по выявлению, анализу, предупреждению и нейтрализации негативных источников, причин и условий воздействия на информацию и на основе этого сформирован механизм комплексного обеспечения цифровой безопасно сти промышленного предприятия в условиях развития цифровой экономики Украины. В рамках разработанного механизма предложено построить эффективную стратегию внедрения и функционирования цифровой безопасности промышленной безопасности на основе определенных базовых универсальных положений этой стратегии. Предложен комплекс практических мер обеспечения реализации стратегии цифровой безопасности промышленного предприятия в режиме непрерывного времени. Сделан вывод, что для современного промышленного предприятия крайне важно сформировать эффективную систему экономической и информационной безопасности, центральным местом которой будет занимать надежная цифровая безопасность..

Ключевые слова: экономическая безопасность; информационная безопасность; цифровая безопасность; цифровая; экономика; кибербезопасность.

N. AVANESOVA, O. MORDOVTSEV, T. KOLODYAZHNA

FORMATION OF A MECHANISM FOR COMPREHENSIVE DIGITAL SECURITY OF AN INDUSTRIAL ENTERPRISE IN UKRAINE

The article deals with theoretical, methodological and practical aspects of integrated digital security as a basis for creating a reliable system of information and economic security within the digital economy at an industrial enterprise in Ukraine. It is found that the digital economy increases the efficiency of all industrial sectors through the use of information technologies; qualitatively and quantitatively increases the ability to carry out almost all economic operations of the economy through a computer. It is determined that the possibility of internal and external interference in the information system of an industrial enterprise can negatively affect the distortion of information parameters such as confidentiality, integrity, availability, reliability, and so on. The analysis of the basic research of the conceptual foundations of the essence of the categories" information security"," cybersecurity "and" digital security "in industrial enterprises is carried out and a generalized definition of the category"digital security" is given. It is proved that the digital security of an industrial enterprise consists in the formation of principles, methods and measures to identify, analyze, prevent and neutralize negative sources, causes and conditions of impact on information.based on this, a mechanism for comprehensive digital security of an industrial enterprise in the context of the development of the digital economy of Ukraine is formed. Within the framework of the developed mechanism, it is proposed to build an effective strategy for the implementation and functioning of digital industrial safety based on certain basic universal provisions of this strategy. A set of practical measures to ensure the implementation of the digital security strategy of an industrial enterprise in continuous time is proposed. It is concluded that it is extremely important for a modern industrial enterprise to form an effective system of economic and information security, the Central place of which will be occupied by reliable digital security.

Keywords: economic security; information security; digital security; digital economy and cyber security.

Вступ Впровадження цифрової економіки в Україні спричинило те, що переважна більшість промислових підприємств стали активними учасниками фінансово-господарських відносин. За допомогою цифрової економіки підвищується ефективність всіх промислових галузей за рахунок використання інформаційних технологій; якісно і кількісно збільшуються можливості здійснення через комп'ютер практично всіх господарчих операцій. Однак слід відзначити, що цифрова трансформація несе й певні ризики. Спотворення або фальсифікація, знищення або розголошення певної частини інформації, так само як й дезорганізація процесів її обробки і передачі, може завдати серйозної матеріальної та моральної шкоди.

Таким чином, вкрай гостро постає питання забезпечення інформаційної та цифрової безпеки крупних промислових підприємств України.

Постановка задачі. Завдання побудови системи цифрової безпеки промислових підприємств має носити комплексний характер. Керівництво та менеджери вищого та середньо ланки мають оцінити рівень передбачуваних ризиків і виробити модель загроз для даного конкретного підприємства. Для забезпечення цифрової безпеки потрібне проведення усестороннього дослідження усіх сфер фінансово-господарчої діяльності промислового підприємства, за результатами якого виробляється комплекс необхідних організаційних і програмно-технічних заходів та способів їх здійснення.

Таким чином, для успішного економічного розвитку промислових підприємств України необхідна розробка комплексного теоретико-методичного забезпечення цифрової безпеки.

Мета роботи. Метою статті є формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України.

Аналіз основних досягнень і літератури.

Теоретико-методологічні засади впровадження та комплексного функціонування цифрової та загальної інформаційної безпеки промислових підприємств опрацьовані в працях таких вчених, як Бурячок В.Л. [1], Горова С. В. [2], Горовий В. [3], Корж І.Ф. [4], Литвиненко О. [5], Лужецький В. А. [6], Марущак А. І. [7], Рубан В.Я. [8], Ткачук Т. Ю. [9], Хаба Р.С. [10], В.Шульга [11].

Треба відзначити, що важливим інформаційно-правовим документом щодо комплексного забезпечення цифрової безпеки промислового підприємства є Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» від 17.01.2018 р. №67-р. В ньому документі визначено засади щодо стимулювання використання цифрових технологій, продуктів та послуг серед суб'єктів економічних відносин України, зростання обсягів виробництва інноваційної продукції промислових підприємств [12]. Але, на законодавчому рівні ще не сформовано поняття «цифрова безпека підприємства»

Разом з тим, можна стверджувати, що спостерігається недостатня кількість проведених досліджень, присвячених проблемам забезпечення цифрової безпеки промислових підприємств. Це виражається в тому .що не отримало належного обґрунтування питання формування та впровадження комплексного механізму функціонування цифрової безпеки як основи для створення системи інформаційної безпеки промислових підприємств.

Викладення основного матеріалу дослідження.

Питання інформаційної, та зокрема цифрової безпеки, вже давно почало входити до числа головних пріоритетів менеджменту всіх великих національних і світових компаній та підприємств, а останніми роками все більше число керівників промислових підприємств України усвідомлювати реальну небезпеку ризиків, пов'язаних з витіком інформації та, як результат, появою інсайдерської інформації.

Можливість внутрішнього та зовнішнього втручання в інформаційну систему промислового підприємства може негативно вплинути на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність тощо. Це приводить до негативних наслідків у діяльності промислового підприємства, а саме:

– збою у функціонуванні систем управління управлінськими та технологічними процесами;

– розголошення інформації, яка є комерційною таємницею;

– порушення достовірності фінансової звітності;

– несанкціонованого доступу до різних баз даних промислового підприємства;

– невірності у викладені публічної інформації

Отже, результатом недостовірної та/або викривленої інформації про діяльність промислового підприємства може стати:

– зменшення вартості власного капіталу підприємства;

– складнощі залучення інвестицій, особливо це стосується іноземних;

– погіршення або навіть розрив ділових відносин із внутрішніми та іноземними партнерами, як із постачальниками, так й із споживачами;

– виникнення проблем у переговорному процесі та, як результат, втрата вигідних контрактів;

– невиконання або недовиконання договірних зобов'язань;

– відмова від рішень, які стали неефективними через розголос інформації;

– неможливість патентування результатів науково-технічної діяльності та продажу ліцензій;

– зниження цін та/або обсягів реалізації;

– нанесення шкоди діловій репутації та авторитету промислового підприємства;

– складнощі в отриманні кредитів на невигідних умовах їх отримання;

– виникнення труднощів в постачанні та придбанні устаткування тощо.

Зазначимо, що у певних ситуаціях нехтування питаннями цифрової безпеки може призвести й до повної втрати бізнесу.

Отже, в загальному сенсі поняття цифрової безпеки можна розглядати у декількох аспектах. На макрорівні, це загальний стан захищеності інформаційно-цифрового середовища країни, який забезпечує його формування, використання й розвиток в інтересах громадян, підприємств та держави. На мікрорівні, це стан захищеності цифрової інформації підприємства, за допомогою якого забезпечується його існування та інноваційний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Для більш чіткого розуміння сутності поняття цифрова безпека необхідно розглянути також споріднені терміни, а саме: «інформаційна безпека» та «кібербезпека». Вони розуміється науковцями по-різному у залежності від потреб їх дослідження, що наглядно продемонстровано у таблиці.

Виходячи із таблиці визначимо, що цифрова безпека є основним компонентом інформаційної безпеки та являє собою комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак і несанкціонованого втручання.

Отже, можна зробити висновок, що цифрова безпека промислового підприємства полягає у формуванні принципів, методів та заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію. Враховуючи це, на рисунку 1 сформуємо механізм комплексного забезпечення цифрової безпеки промислового підприємства в умовах розвитку цифрової економіки України (рис.).

Таблиця – Основні визначення понять «інформаційна безпека», «кібербезпека» та «цифрова безпека»

Автор	Визначення
Бурячок В.Л. [1]	кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам
Горова С. В. [2]	стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку, незалежно від впливу внутрішніх і зовнішніх інформаційних загроз»
Корж І.Ф. [3]	інформаційна безпека – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення і прав суб’єктів, що беруть участь в інформаційній діяльності
Литвинов О. [4]	під інформаційною безпекою варто розуміти одну зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами
Лужецький В. А. [5]	інформаційна безпека – це стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства
Марущак А. І. [6]	розглядає інформаційну безпеку та, зокрема, елементи цифрової безпеки, як стан захищеності життєво важливих інтересів підприємства, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації
Рубан В.Я. [7]	під інформаційною безпекою розуміє необхідність протидії витоку інформації з обмеженим доступом, а також поширенню недостовірної інформації, однак застосування системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від побутового
Саврук М.В. [8]	цифрова безпека – це стан захищеності інформації, яка забезпечує життєво важливі інтереси підприємства та суспільства в цілому
Ткачук Т. Ю. [9]	Визначає цифрову безпеку як безпеку об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією, та нерозголошення даних про той чи інший об’єкт, що є комерційною таємницею
Хаба Р.С. [10]	пропонує визначати інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, котрі являють собою впорядковану сукупність як інформаційних ресурсів (не лише держави, а й фізичних та юридичних осіб), так і інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі. Встановлення та функціонування вказаної системи засобів спрямоване на забезпечення прав людини, інтересів суспільства та держави в інформаційній сфері
Шульга В. [11]	пропонує інформаційну безпеку розглядати через єдність таких ознак, як стан, властивість управління загрозами й небезпеками. Ці чинники забезпечують обрання оптимального шляху усунення загроз та мінімізації впливу негативних наслідків

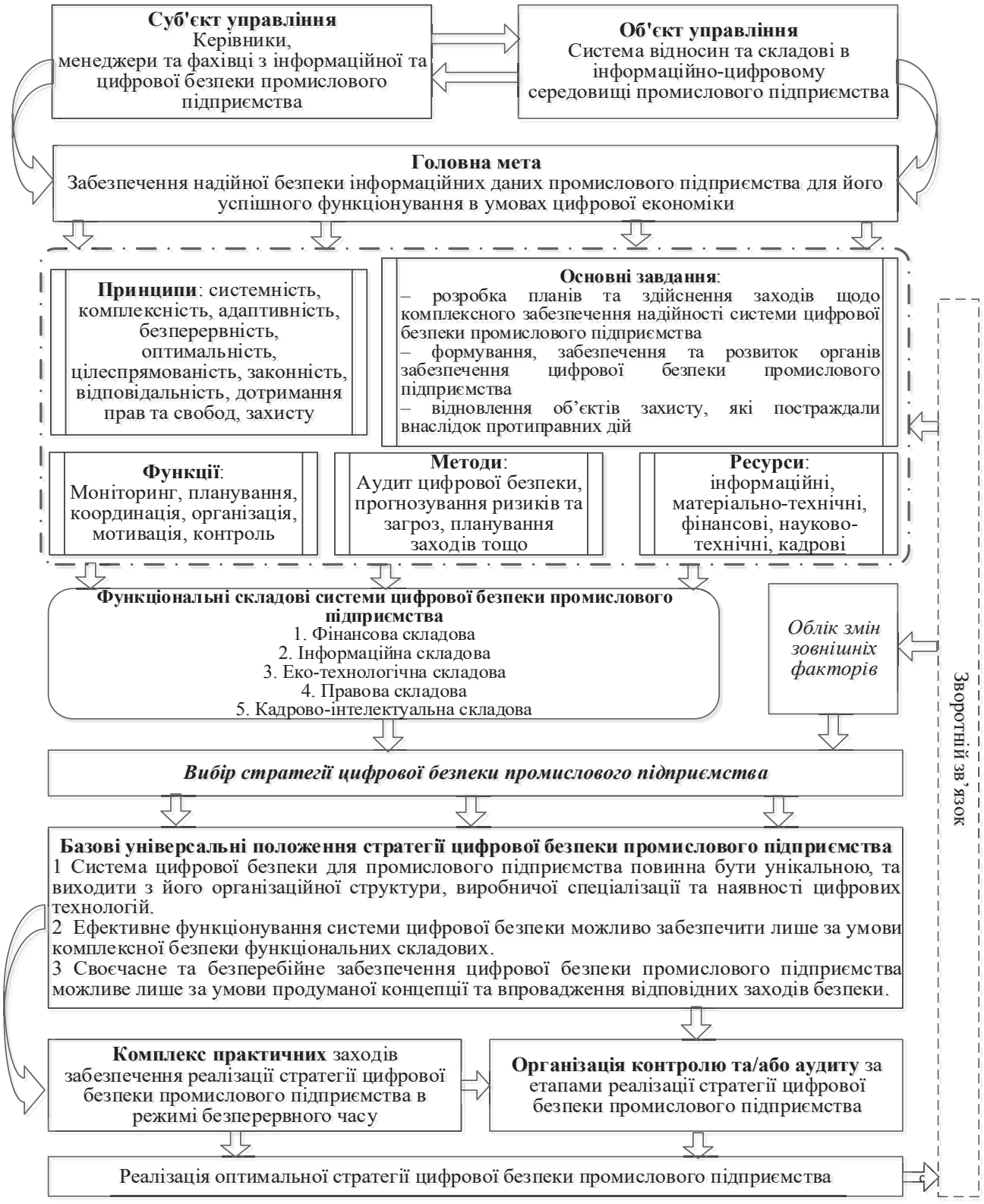

Рисунок – Механізм комплексного забезпечення цифрової безпеки промислового підприємства України

Розглянемо більш детально окремі елементи механізму комплексного забезпечення цифрової безпеки промислового підприємства України (рис.). Зазначимо, що він повинен базуватися на наступних принципах:

– системності – цей принцип базується на засадах багатоскладової, цілісної, відкрито-динамічної системи із структурно побудованою системою підпорядкування окремих елементів, які у режимі реального часу взаємодіють один з іншим, з мікросередовищем та макросередовищем, а також здійснює вплив на усі аспекти цифрової безпеки промислового підприємства;

– комплексності – розроблений механізм повинен мати відповідний набір базових комплексних показників, які, у подальшому, можуть використовуватися на усіх етапах впровадження та ефективного застосування цифрової безпеки;

– безперервності – згідно цього принципу промислове підприємство повинно постійно нарощувати потенціал цифрової безпеки на засадах створення ефективно стратегії для підвищення конкурентоспроможності в умовах роботи у цифровій економіки;

– оптимальності – означає, що усі рішення при впроваджені цифрової безпеки має бути найкращими за вибраними у системі критеріями та відповідати поставленої меті промислового підприємства. Вибір оптимального критерію багатогранний та складний процес, який потребує залучення різних методів і моделей, а також комунікації між різними суб’єктами інформаційної та загальної економічної безпеки підприємства;

– цілеспрямованості – сутність цього принципу полягає у спрямовуванні діяльності промислового підприємства на досягнення загальних цілей та виконання поставлених планових завдань щодо забезпечення належного рівня цифрової безпеки промислового підприємства;

– законність – сутність цього принципу полягає у дотриманні законів України при впровадженні заходів цифрової безпеки на підприємстві;

– відповідальність – означає, що кожен керівник та менеджер, який відповідає за сегмент безпеки, повинен докладати усіх зусиль для ефективізації заходів цифрової безпеки та недопущення втрати або пошкодження інформаційних даних;

– дотримання прав та свобод та захисту – ці принципи загальноприйняті та діють на усі процеси економічної безпеки промислового підприємства.

Базисом для створення ефективної системи цифрової безпеки промислового підприємства є наступні ресурси:

— інформаційні ресурси – це сукупність інформації, яка є основним джерелом для створення надійної системи цифрової безпеки промислового підприємства. Без наявності повної, достовірної, своєчасної, диференційованої та потенціальної інформації неможливо впровадити ефективну систему інформаційної безпеки. Також, слід відзначити, що інформаційні ресурси можуть транспонуватися у інформаційний потенціал, який характеризується перспективною складовою використання цього ресурсу;

– матеріально-технічні ресурси – спеціальні комп’ютери та обладнання к ним, програмне забезпечення тощо;

– фінансові ресурси – це грошові кошти, які повинні виділятися промисловим підприємством на заходи цифрової безпеки;

– науково-технічні ресурси дозволяють створювати та впроваджувати нові технологій у сфері інформаційної та цифрової безпеки.

Серед основних функцій створеного механізму особливої уваги заслуговує моніторинг, тобто комплекс дій, який повинен використовуватися для забезпечення керівництва базисною інформацією про усі аспекти цифрової безпеки та можливості побудови ефективної системи її безперебійного функціонування в умовах цифрової економіки.

Ключовим фактором успішності створення системи цифрової безпеки промислового підприємства є побудова ефективної стратегії її впровадження та функціонування на засадах визначених базових універсальних положень цієї стратегії. Але, треба відзначити, що ці положення є лише загальними рекомендаціями, та не є аксіомою для конкретного підприємства. Тому в представленому у дослідженні механізмі пропонується використовувати комплекс практичних заходів забезпечення реалізації стратегії цифрової безпеки промислового підприємства в режимі безперервного часу, а саме;

– використання лише ліцензійного програмного забезпечення та програм;

– регулярне оновлення усього програмного забезпечення;

– встановлення антивірусних програм та «firewall» (антивірус захищає комп’ютер від вірусів, а фаєрвол відслідковує міжмережеві зв’язки комп’ютера та мережі Інтернет і, відповідно, захищає від загроз ззовні);

– встановлення унікальних, складних паролів на вхід у корпоративні комп’ютери та інші пристрої підприємства (цим правилом часто нехтують менеджери промислових підприємств та встановлюють стандартні паролі);

– використання менеджеру паролів для уникнення складнощів у пошуку потрібних паролів у випадку їх втрати;

– використання лише надійних поштових сервісів, соціальних мереж та месенджери (це ж стосується й заборонених законодавством України)

– розділення облікових записів різних процесів та сегментів діяльності промислового підприємства для ускладнення взлому та втрати інформаційних даних;

– видалення історії з браузерів та кеш. При роботі в Інтернеті, то сайти, на які ви заходите, відправляють на ваш комп’ютер невеличкі файли, щоб знати, що це були ви, та відповідно індексують усі ваші дії та можуть потенційно завдати школи або слідкувати за важливою інформацією. Рекомендовано використовувати програму CCleaner або її аналоги;

– заборонено використовувати для відновлення доступу у корпоративні поштові незахищені поштові скриньки.

– використання лише секретних месенджерів для проведення кондиційної переписку;

– категорична заборона «клікати» на підозрілі посилання з корпоративних комп’ютерів для запобігання втрати або пошкодження важливої інформації;

– робити комплекс дій щодо запобігання фішингу, тобто виду шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо;

– робити резервні копії важливих файлів в хмарних сховищах. Хмарні сховища – це Google Диск, Dropbox. Статистично є дуже ймовірним, що може трапитись пошкодження жорсткого диску або флешки без можливості відновлення.

– зробити двофакторну авторизацію (корпоративні телефоні номери) для важливих облікових записів.

– використання технології VPN (Virtual Private Network — віртуальна приватна мережа) або мережу Tor (The Onion Router) у випадках коли потрібно додатковий захист інформації у публічних мережах та засадах анонімності;

– змінення дефолтних паролів Wi-Fi-роутерів (паролі за замовчуванням).

Висновки. У ході проведеного дослідження щодо формування універсального механізму комплексного забезпечення цифрової безпеки промислового підприємства України було:

1 Уточнено сутність категорії «цифрова безпека» підприємства та виявлено, що немає її єдиного та канонічного трактування. Тому у досліджені запропоновано трактувати цифрову безпеку промислового підприємства як комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак і несанкціонованого втручання

2 Сформовано універсальний механізм комплексного забезпечення цифрової безпеки промислового підприємства в умовах розвитку цифрової економіки України та доведено, що динамічний розвиток підприємства неможливий без практичного його використання. В рамках розробленого механізму надані універсальні та практичні заходи щодо удосконалення системи цифрової, інформаційної та загалом економічної безпеки промислового підприємства.

Отже, можна зробити висновок, що для сучасного промислового підприємства вкрай важливо сформувати ефективну систему економічної та інформаційної безпеки, центральним елементом якої буде стратегічна та надійна цифрова безпека.

Список літератури

1. Бурячок В.Л. *Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби*. Київ : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.
2. Горова С.В. *Особа в інформаційному суспільстві: виклики сьогодення*. Київ : ТОВ «СІК ГРУП УКРАЇНА», 2017. 452 с.
3. Корж І.Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук-практ. конф. 06 жовт. 2016 р.* Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. 204 с.
4. Литвинов В.В. *Моделювання та аналіз безпеки розподілених інформаційних систем*. Чернігів : нац. технол. ун-т, 2016. 254 с.
5. Лужецький В.А., Войнович О.П., Дудатьєв А.В. *Інформаційна безпека*. Вінниця : УНІВЕРСУМ-Вінниця, 2012. 240 с.
6. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92-95.
7. Рубан В.Я. Інформаційна безпека України: сутність та проблеми. *Стратегічна панорама*. 2008. № 3-4. С. 170-175
8. Саврук М.В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. *Системи обробки інформації*. 2010. №3(84). С. 77-79.
9. Ткачук Т.Ю. Інформаційна безпека держави у національному законодавстві європейських країн. *Visegrad Journal on Human Rights*. 2018. № 1. С. 145–150.
10. Хаба Р.С. Деструктивні інформаційні впливи в сучасних умовах. *Інформаційна безпека людини, суспільства, держави*. 2017. №1(21). С. 216-224
11. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 20.08.2020)
12. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 рр. та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету міністрів України від 17.01.2018 р. №67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80/.(дата звернення: 20.08.2020)

References (transliterated)

1. Buriachok V. *Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby* [Information and cyberspace: security problems, methods and means of struggle]. Kiev, TOV «SIK HRUP UKRAINA», 2015. 449 p.
2. Horova S. *Osoba v informatsiinomu suspilstv i: vyklyky sohodennia* [Face in the information society: challenges of the present], Kiev, TOV «SIK HRUP UKRAINA», 2017. 452 p.
3. Korzh I. Vnutrishni faktory zahroz i vyklykiv informatsiinii bezpetsi Ukrainy [Internal factors of threats and challenges to information security of Ukraine]. *Zapobihannia novym vyklykam ta zahrozam informatsiinii bezpetsi Ukrainy: pravovi aspekty : materialy nauk.-prakt. konf. 06 zhovt. 2016 r.* [Prevention of new challenges and threats to information security in Ukraine: legal aspects: materials of science-practice Conf. 06 Oct. 2016]. Kiev, NTUU «KPI imeni Ihoria Sikorskoho», Vyd-vo «Politekhnika», 2016. 204 p.
4. Lytvynov V. Modeliuvannia ta analiz bezpeky rozpodilenykh informatsiinykh system [Modeling and analysis of security of distributed information systems]. Chernihiv, nats. tekhnol. un-t, 2016. 254 p.
5. Luzhetskyi V., Voinovych O., Dudatiev A. *Informatsiina bezpeka* [Information security]. Vinnytsia, UNIVERSUM-Vinnytsia, 2012. 240 p.
6. Marushchak A. Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky [Information and legal directions of research of problems of information security]. *Derzhavna bezpeka Ukrainy* [State security of Ukraine]. 2011. vol. 21. pp. 92-95.
7. Ruban V.. Informatsiina bezpeka Ukrainy: sutnist ta problem [Information security of Ukraine: the essence of the problem]. *Stratehichna panorama* [Strategic panorama]. 2008. vol. 3-4. pp. 170-175
8. Savruk M. Aktualnist problemy zabezpechennia informatsiinoi bezpeky Ukrainy ta shliakhy yii rozviazannia systemy obrobky informatsii [Relevance of the problem of ensuring information security in Ukraine and ways to solve it information processing systems]. *Systemy obrobky informatsii* [Information processing system]. 2018. vol. 1. pp. 145–150.
9. Tkachuk T. Informatsiina bezpeka derzhavy u natsionalnomu zakonodavstvi yevropeiskykh krain [Information security of the state in the national legislation of European countries]. *Visegrad Journal on Human Rights* [Visegrad Journal on Human Rights]. 2018. vol. 1. pp. 145-150.
10. Khaba R. Destruktyvni informatsiini vplyvy v suchasnykh umovakh [Destructive information impacts in modern conditions]. C*Informatsiina bezpeka liudyny, suspilstva, derzhavy* [Inf ormation security of a person, society, and state]. 2017. vol.1(21). pp. 216-224
11. Shulha V. Suchasni pidkhody do traktuvannia poniattia informatsiina bezpeka [Modern approaches to the interpretation of the concept of information security]. *Efektyvna ekonomika* [Efficient economy]. 2015. vol. 4. Available at: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80/. (accessed 20.08.2020).
12. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 rr. ta zatverdzhennia planu zakhodiv shchodo yii realizatsii : *Rozporiadzhennia Kabinetu ministriv Ukrainy vid 17.01.2018 r. №67-r*. Available at: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80/ (accessed 20.08.2020).

Надійшла (received) 03.06.2020

Відомості про авторів / Сведения об авторах / About the Authors

Аванесова Ніна Едуардівна (Аванесова Нина Эдуардовна, Avanesova Nina) – доктор економічних наук, професор, Харківський національний університет будівництва та архітектури, завідувач кафедри менеджменту та публічного адміністрування, м. Харків, Україна, ORCID: https://orcid.org/0000-0003-3636-9769 e-mail: Avanesova.science@gmail.com

Мордовцев Олександр Сергійович (Мордовцев Александр Сергеевич, Mordovtsev Oleksandr) – кандидат економічних наук, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри міжнародного бізнесу та фінансів; м. Харків, Україна, ORCID: https://orcid.org/0000-0003-1653-5440; e-mail: acmordov@gmail.com

Колодяжна Тетяна Вікторівна (Колодяжная Татьяна Викторовна, Kolodyazhna Tetyana) – кандидат економічних наук, Харківський національний університет будівництва та архітектури, доцент кафедри фінансів та кредиту, м. Харків, Україна, ORCID: https://orcid.org/0000-0002-1921-5744, e-mail: Kolodyazhna.t@gmail.com