MANAGEMENT

УДК 338.242(477)
JEL B41, E60, H11, H56 DOI: https://doi.org/10.26906/EiR.2022.3(86).2817

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ СТРАТЕГІЧНО ВАЖЛИВИХ ПІДПРИЄМСТВ В УМОВАХ ВИКЛИКІВ Й ЗАГРОЗ

Онищенко Світлана Володимирівна*, доктор економічних наук, професор
Ківшик Олександр Петрович, докторант**
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

**ORCID 0000-0002-6173-4361*
***ORCID 0000-0002-7154-2603*

© Онищенко С.В., 2022
© Ківшик О.П., 2022

Стаття отримана редакцією 24.11.2022 р.
The article was received by editorial board on 24.11.2022

Вступ. Відкрита та широкомасштабна війна росії у XXI ст. зумовила нові реалії й нові безпекові виклики в світі. Глобальний масштаб загроз та небезпек вимагають невідкладних структурних змін національної економіки у воєнний період. Водночас, процеси цифровізації збільшили появу нових інформаційних загроз та масштабних кібератак від рф й виявили критичні проблеми в інформаційній безпеці. Всі ці загрози зумовлюють формування системи безпекоорієнтованого інформаційного середовища як для суб'єкта господарювання, стратегічних галузей, так і для зміцнення національної безпеки в цілому. Критично важливим та своєчасним є дослідження управління інформаційною безпекою стратегічно важливих підприємств, котрі включають, насамперед, підприємства в таких сферах, як оборона, паливно-енергетичний комплекс, транспорт та зв'язок, АПК, фінансово-бюджетна сфера тощо.

Огляд останніх джерел досліджень і публікацій. Значна частина досліджень управління інформаційною безпекою підприємств, в тому числі у контексті підтримки національної безпеки країни, широко актуалізуються у працях зарубіжних та вітчизняних науковців. В умовах поглиблення процесів цифровізації наукові дослідження присвячуються розробленню напрямів упередження й мінімізації загроз інформаційній безпеці, зміцнення захищеності суб'єктів господарювання в інформаційному просторі [1–6]. Водночас, визначення особливостей стратегічно важливих підприємств, як основи безпеки національної економіки, удосконалення їх інституційного забезпечення, а також проблематика приватизації та реформування стратегічно важливих підприємств активно досліджується вітчизняними науковцями [7–8] в аспекті критичної необхідності зміцнення безпеки України в умовах викликів та загроз.

Відокремлення невирішених раніше частин загальної проблеми. В умовах військової агресії російської федерації при постійному зростанні викликів у інформаційному й кіберпросторі проблема управління підприємствами, що мають стратегічне значення для економіки і безпеки держави є актуальною й потребує подальшого дослідження.

Метою статті є поглиблення проблематики управління інформаційною безпекою стратегічно важливих підприємств в умовах воєнного стану.

Основний матеріал і результати. Війна є масштабним структурним шоком для економіки України, одним із проявів якого стала втрата державним бюджетом значної частини традиційних надходжень у вигляді податків, акцизів та митних платежів. Частина цих втрат замінена пільговим фінансуванням від

міжнародних партнерів та прямим фінансуванням бюджету центральним банком, що має інфляційний та девальваційний ефект, але надзвичайні обставини вимагають надзвичайної реакції. Іншими словами, в умовах війни… «ми не питаємо, як ми будемо платити за неї – ми це вирішуватимемо після її завершення» [9].

Міністерство економіки попередньо оцінило падіння ВВП України за підсумками 2022 року на рівні 30,4%. Важливість безпечного існування національної економіки актуалізується потребою хоча б часткового відновлення реального сектору економіки й особливо підприємств, що мають стратегічне значення для економіки і безпеки держави.

Відновлення реального сектору економіки залежить від стану розвитку стратегічних галузей та їх безпечного функціонування. Зміст поняття «стратегічні галузі» вживаються, в контексті національних економічних інтересів, і ототожнюються з «пріоритетні» – щодо стимулювання інноваційної чи інвестиційної діяльності (зокрема, у 2013 р. пріоритетними були визнані в Україні деякі напрями агропромислового, житлово-комунального та машинобудівельного комплексів, а також транспортної інфраструктури, курортно рекреаційної сфер та і туризму та переробної промисловості [10]).

Досліджуючи законодавче забезпечення статусу «стратегічні галузі» маємо нагальну потребу унормувати та інституційно визначити перелік стратегічних галузей, особливо військово-промислового комплексу, паливно-енергетичного комплексу, транспорту та зв'язку, агропромислового комплексу й інших, враховуючи їх значення для економіки і безпеки держави. Розвиток та функціонування стратегічних галузей України залежить від ефективності діяльності підприємств, які мають стратегічно важливе значення для економіки і безпеки держави (далі – стратегічно важливих підприємств).

В Україні сутність та зміст поняття «стратегічно важливі підприємства для економіки та безпеки держави» офіційно не визначено, а існує лише ситуаційно сформований перелік таких підприємств. Постановами Кабінету Міністрів України визначено критерії віднесення об'єктів державної власності до таких, що мають стратегічне значення для економіки і безпеки держави [11] затверджено перелік об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави [12].

Член-кореспондент НАН України Манцуров І. наголошує, що подолання кризових явищ в економіці та забезпечення динамічного соціально-економічного розвитку країни можливе через використання потенціалу та посилення уваги до стратегічно важливих підприємств. В аспекті реалізації національних інтересів, поряд з розвитком стратегічних галузей, доцільно враховувати також функціонування стратегічно важливих підприємств, котрі їх органічно доповнюють та деталізують. Це вмотивовано тим, що, по-перше, навіть у складі стратегічних галузей можна виокремити ті підприємства, які визначають їх розвиток, а по-друге, стратегічні підприємства можуть функціонувати у сферах, що не визначені як стратегічні, але при цьому суттєво впливають на різні складові економічної безпеки (виробничої, фінансової, соціальної тощо) [7].

Враховуючи реалії сьогодення потрібно не тільки визначити статус стратегічно важливих підприємств, а й законодавчо закріпити можливість здійснювати урядовий контроль за діяльністю стратегічних для держави підприємницьких структур.

Стратегічно важливі підприємства та об'єкти критичної інфраструктури повинні мати найвищий ступінь захисту інформації. Інформаційна безпека цих підприємств характеризує стан їх доступу до інформації, її захищеності, зберігання, ефективності використання, проведення ділової розвідки, інформаційно-аналітичної роботи із зовнішніми та внутрішніми суб'єктами, здатність інформаційно-аналітичної системи суб'єктів господарювання до розвитку.

Дослідження існуючої нормативно-правової бази України щодо кіберзахисту державних інформаційних ресурсів свідчить про те, що уніфікація чималої кількості діючих керівних нормативно-правових документів та стандартів відбувається з урахуванням норм міжнародного права, галузевих стандартів та директив ЄС та НАТО, що зафіксовано у Законах та нормативно-правовій базі України [2; 4; 13].

Загальні положення інформаційної безпеки формалізовані й закріплені у Стратегії інформаційної безпеки, відповідно до якої інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі

скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [14].

Система аналітичної інформації для прийняття управлінських рішень характеризується складністю. Причому спостерігається тенденція до ускладнення взаємозв'язків в інформаційному потоці. Одночасно відбувається систематичне зростання обсягів інформації, її надмірності при інформаційній недостатності для прийняття оптимальних управлінських рішень. Інформація щодо забезпечення безпеки суб'єктів підприємництва досить неоднорідна [15]. Усе це ускладнює її використання в управлінні безпекою та забезпеченням життєздатності суб'єкта господарювання.

Водночас, більшість заходів щодо оцінки захищеності систем відрізняються досить великими обсягами. Багато програм захисту створено власними силами цих підприємств та установ, навіть сучасні методи та засоби інформаційно-комунікаційних та цифрових технологій не можуть в повній мірі забезпечити продуктивну та надійну обробку постійно зростаючих масивів інформації. Існуюча позиційна двійкова система числення, що функціонує в сучасних інформаційних технологіях, має недоліки [3], а існуючі методи несанкціонованого доступу, хакерські атаки, віруси та інші види злому та порушення цілісності інформації побудовані з використанням двійкового позиційного коду.

Управління інформаційною безпекою стратегічно важливих підприємств, особливо в умовах воєнного стану безумовно являється основною детермінантою забезпечення стабільного функціонування галузей національної економіки України. Необхідність формування інформаційної безпеки зумовлюється наявністю загроз та їх деструктивними наслідками. З метою своєчасного виявлення, унеможливлення реалізації, мінімізації негативного впливу загроз інформаційній безпеці необхідним є їх оперативна ідентифікація.

Систематизацію загроз інформаційній безпеці стратегічно важливих підприємств доцільно здійснювати з урахуванням чинного законодавства.

У Стратегії національної безпеки України виокремлено ряд поточних і прогнозованих загроз національній безпеці та національним економічним інтересам. Згідно зі Стратегією загрозами інформаційній безпеці стратегічно важливих підприємств правомірно визначити стрімкий розвиток інформаційних технологій, що є причиною поширенню злочинності у кіберпросторі та деструктивної пропаганди в інформаційному середовищі; слабкість системи стратегічних комунікацій; зростання несанкціонованих втручань кіберхарактеру в функціонування об'єктів критичної інфраструктури; відсутність цілісної інформаційної політики держави [16].

Згідно зі Стратегією інформаційної безпеки загрози інформаційній безпеці стратегічно важливих підприємств доцільно поділяти за рівнем реалізації на глобальні та національні. До глобальних загроз правомірно віднести збільшення кількості глобальних дезінформаційних кампаній та їх деструктивного впливу у національному та світовому інформаційному просторі; розгорнуту рф кібервійну проти України та інших демократичних країн, що супроводжується кібератаками на стратегічно важливі підприємства та об'єкти критичної інфраструктури; недостатній рівень обізнаності суб'єктів господарювання в питанні забезпечення інформаційної безпеки в умовах стрімкого розвитку цифрових технологій. Національні загрози включають відсутність в Україні ефективної система реагування на кібервиклики; несформованість системи стратегічних комунікацій; відсутність ефективних систем захисту інформації на рівні суб'єктів господарювання [14].

Відповідно до Стратегії кібербезпеки України доцільно виокремити такі види загроз інформаційній безпеці стратегічно важливих підприємств як кібервійна, кібертероризм, кіберзлочинність, кібершпигунство [17].

Враховуючи положення розглянутих стратегій, вважаємо доречним доповнити розподіл загроз інформаційній безпеці стратегічно важливих підприємств за ступенем детермінізму: випадкові загрози – загрози, які можуть бути реалізовані або не відбутися; закономірні загрози – загрози, які мають стійкий, повторюваний характер та зумовлені об'єктивними умовами розвитку цифровізації та посилення напруги на світовій арені [5; 18].

Доцільно також доповнити класифікацію загроз інформаційній безпеці стратегічно важливих підприємств поділом за об'єктами дестабілізуючих дій, що дозволить визначити важелі та інструменти побудови ефективної системи захисту інформаційних ресурсів на різних рівнях – на рівні держави, регіону (галузі), підприємства, особи (домогосподарства).

Доповнену систематизацію загроз інформаційній безпеці правомірно визначити базисом для формування напрямів їх запобігання і протидії та побудови ефективної системи управління інформаційною безпекою стратегічно важливих підприємств в цілому.

Висновки. На основі проведеного дослідження доцільно зробити наступні висновки:

1. Відновлення реального сектору економіки України у повоєнний період залежить від стабільного та безпечного функціонування стратегічних галузей, тому нагальною визначена потреба унормувати та інституційно визначити перелік стратегічних галузей.

2. Враховуючи вплив стратегічно важливих підприємств на економічну та національну безпеку країни в цілому, необхідно визначити статус стратегічно важливих підприємств та законодавчо закріпити можливість здійснювати урядовий контроль за діяльністю стратегічних для держави підприємницьких структур.

3. В умовах цифровізації, яка спричинила появу нових ризиків і загроз функціонуванню національних економік та виявила критичні проблеми в інформаційній сфері, забезпечення інформаційної безпеки є необхідною умовою стабільного функціонування не тільки стратегічно важливих підприємств, а й стратегічних галузей в цілому. Побудова надійної системи захисту інформації має ґрунтуватися на своєчасній ідентифікації загроз інформаційній безпеці.

4. Систематизація загроз інформаційній безпеці стратегічно важливих підприємств з урахуванням положень чинного законодавства правомірно визначена основою їх запобігання та базисом для прийняття ефективних управлінських рішень щодо забезпечення функціонування стратегічно важливих підприємств на засадах інформаційної захищеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Lytvynenko O. Information component in the modern hybrid war against Ukraine: challenges and threats. *Ukrainian Studies Almanac*. 2017. Issue 19, 171–174.
2. Данілов О. Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни. 2020. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html
3. Glushko A.D., Yanko A.S. Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. *Economics and Region*. 2019. No. 4 (75). P. 20–28. https://doi.org/10.26906/eip.2019.4(75).1814
4. Петров В. Важливість захисту національних інтересів держави в інформаційному просторі. 2021. URL: https://bintel.org.ua/analytics/voenni-voprosy/armii-voorugenie/konceptualni-zasadu-proyektu-strategii-kiberbezpeki-ukraini-na-2021-2025-roki/
5. Шемчук В.В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*. 2020. № 1(7). С. 285–296. DOI: https://doi.org/10.32689/2617-9660-2020-1(7)-285-296
6. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management*. 2020. Vol. 18, Issue 3, 195–210.
7. Манцуров І., Рудченко О., Новиков В. Феномен стратегічно важливих підприємств в Україні. *Україна: аспекти праці. Серія: економіка державного сектору.* 2017. № 3. С. 44–51.
8. Баланда А.Л., Павленко В.П., Рудченко О.Ю. Інституційне забезпечення державного регулювання стратегічно важливих підприємств для економіки та безпеки держави. *Формування ринкових відносин в Україні : зб. наук. пр.* Вип. 5. (180). Київ, 2016. С. 18–22.
9. When the war is over: необхідні кроки з економічного відновлення України. URL: https://lb-ua.translate.goog/blog/ievhen-stepaniuk/509330_when_war_over_neobhidni_kroki_z.html?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=op,sc
10. Розпорядження Кабінету Міністрів України «Про затвердження переліку пріоритетних галузей економіки» від 14.08.2013 № 843. URL: http://zakon.rada.gov.ua/laws/show/8432013p
11. Постанова Кабінету Міністрів України «Про визначення критеріїв віднесення об'єктів державної власності до таких, що мають стратегічне значення для економіки і безпеки держави» від 03.11.2010 р. URL: https://zakon.rada.gov.ua/laws/show/999-2010-%D0%BF#Text
12. Постанова Кабінету Міністрів України «Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави» від 04.03.2015 р. URL: https://ips.ligazakon.net/document/KP150083?an=1
13. Постанова кабінету міністрів України «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text
14. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/ 2021#Text

15. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. ХНУ, 2020. Вип. 59. С. 14–24.

16. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

17. Стратегії кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

18. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20.

REFERENCES:

1. Lytvynenko, O. (2017) Information component in the modern hybrid war against Ukraine: challenges and threats. *Ukrainian Studies Almanac*. Issue 19, 171–174.

2. Danilov, O. (2020) Cybersecurity of state information resources is an important component of the country's digital transformation. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html

3. Glushko, A.D., Yanko, A.S.(2019) Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. *Economics and Region*. No. 4 (75). P. 20–28. DOI: https://doi.org/10.26906/eip.2019.4(75).1814

4. Petrov, V. (2021) The importance of protecting the state's national interests in the information space. URL: https://bintel.org.ua/analytics/voenni-voprosy/armii-voorugenie/konceptualni-zasadu-proyektu-strategii-kiberbezpeki-ukraini-na-2021-2025-roki/

5. Shemchuk, V.V. (2020). Threats to information security: problems of definition and overcoming [Zahrozy informatsiinii bezpetsi: problemy vyznachennia ta podolannia]. *Expert: paradigms of legal sciences and public administration*. No. 1(7). P. 285–296. DOI: https://doi.org/10.32689/2617-9660-2020-1(7)-285-296

6. Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*. Vol. 18, Issue 3, 195–210

7. Mantsurov, I., Rudchenko, O., Novikov, V. (2017) The phenomenon of strategically important enterprises in Ukraine [Fenomen stratehichno vazhlyvykh pidpryiemstv v Ukraini]. *Ukraine: aspects of labor. Series: Public Sector Economics.* № 3. P. 44–51.

8. Balanda, A.L., Pavlenko, V.P., Rudchenko, O.Yu. (2016) Institutional support of state regulation of strategically important enterprises for the economy and security of the state. *Formation of market relations in Ukraine: a collection of scientific papers*. [Instytutsiine zabezpechennia derzhavnoho rehuliuvannia stratehichno vazhlyvykh pidpryiemstv dlia ekonomiky ta bezpeky derzhavy]. Issue. 5. (180). P. 18–22.

9. When the war is over: necessary steps for Ukraine's economic recovery. URL: https://lb-ua.translate.goog/blog/ievhen-stepaniuk/509330_when_war_over_neobhidni_kroki_z.html?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=op,sc

10. On approval of the list of priority sectors of the economy: Order of the Cabinet of Ministers of Ukraine dated August 14, 2013, No. 843. URL: http://zakon.rada.gov.ua/laws/show/8432013p

11. On determining the criteria for classifying state-owned property as being of strategic importance for the economy and security of the state: Decree of the Cabinet of Ministers of Ukraine dated November 3, 2010. URL: https://zakon.rada.gov.ua/laws/show/999-2010-%D0%BF#Text

12. On approval of the list of state-owned objects of strategic importance for the economy and security of the state: Decree of the Cabinet of Ministers of Ukraine dated March 4, 2015. URL: https://ips.ligazakon.net/document/KP150083?an=1

13. On Approval of the Procedure for Reviewing the State of Cybersecurity of Critical Information Infrastructure, State Information Resources and Information Required to be Protected by Law: Decree of the Cabinet of Ministers of Ukraine dated November 11, 2020, No. 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

14. Information security strategy: Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

15. Onyshchenko, S., Hlushko, A. (2020). Conceptual principles of information security of the national economy in conditions of digitalization [Kontseptualni zasady informatsiinoi bezpeky natsionalnoi ekonomiky v umovakh didzhytalizatsii]. *Social economy: Science. profession. view.* Kh.: KhNU, 59, pp. 14–24. DOI: https://doi.org/10.26565/2524-2547-2020-59-02

16. National Security Strategy of Ukraine: Decree of the President of Ukraine dated 14 September 2020 No. 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

17. Cybersecurity strategies of Ukraine: Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

18. Onyshchenko, S.V., Glushko, A.D. (2022) Analytical dimension of cybersecurity of Ukraine in the context of growing challenges and threats [Analitychnyi vymir kiberbezpeky Ukrainy v umovakh zrostannia vyklykiv ta zahroz]. *Economy and region*. No. 1 (84). P. 13–20.

УДК 338.242(477)
JEL B41, E60, H11, H56

Онищенко Світлана Володимирівна, доктор економічних наук, професор. **Ківшик Олександр Петрович**, докторант, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Управління інформаційною безпекою стратегічно важливих підприємств в умовах викликів й загроз.**

У статті обґрунтовано важливість управління інформаційною безпекою підприємств, що мають стратегічне значення для економіки і безпеки держави. Враховуючи сучасні реалії війни національна економіка переживає масштабний шок, тому необхідно застосовувати комплекс інформаційних, організаційно-економічних та правових заходів щодо відновлення цілих галузей. Першочергової уваги потребують підприємства, які мають стратегічне значення для економіки і безпеки України. Саме тому в дослідженні доведено роль безпекоорієнтованої діяльності стратегічно важливих підприємств у воєнний період та повоєнної відбудови України. Розглянуто загрози інформаційної безпеки стратегічно важливих підприємств. Запропоновано застосування інституційного підходу в управлінні інформаційною безпекою стратегічно важливих підприємств.

Ключові слова: інформаційна безпека, стратегічно важливі підприємства, безпекоорієнтована діяльність, загрози.

UDC 338.242(477)
JEL B41, E60, H11, H56

Svitlana Onyshchenko, Doctor of Economics, Professor. **Oleksandr Kivshyk**, Doctoral student, National University «Yuri Kondratyuk Poltava Polytechnic». **Information security management of strategically important enterprises in the conditions of challenges and threats.**

The article substantiates the importance of managing information security of enterprises of strategic importance for the economy and security of the state. Considering the current realities of the war, the national economy is experiencing a large-scale shock, and therefore it is necessary to apply a set of information, organizational, economic and legal measures to restore entire industries. The authors substantiates the need to regulate and institutionally define the list of strategic industries, on the stable and secure functioning of which the recovery of the real sector of Ukraine's economy in the post-war period will depend. In terms of realization of national interests, along with the development of strategic industries, it is advisable to take into account the functioning of strategically important enterprises that organically complement and detail them. Given the impact of strategically important enterprises on the economic and national security of the country as a whole, the author proposes to define the status of strategically important enterprises and to legislate for the possibility of state control over the activities of business entities of strategic importance to the state. The research proves the role of security-oriented activities of strategically important enterprises during the wartime period and post-war reconstruction of Ukraine. The authors focus on the fact that in the context of digitalization, which has led to the emergence of new risks and threats to the functioning of national economies and revealed critical problems in the information sphere, ensuring information security is a prerequisite for the stable functioning of strategically important enterprises. The application of an institutional approach to the management of information security of strategically important enterprises is proposed. It is proved that building a reliable information security system should be based on timely identification of threats to information security. The systematization of threats to information security of strategically important enterprises, taking into account the provisions of current legislation, is rightly determined as the basis for their prevention and the basis for making effective management decisions to ensure the functioning of strategically important enterprises on the basis of information security.

Key words: information security, strategically important enterprises, security-oriented activities, threats.