УДК 338.43:338.246.87:004.056.5

Л. А. Бехтер,
к. е. н., доцент кафедри управління фінансово-економічною безпекою і проектами,
Запорізький національний університет, м. Запоріжжя
ORCID ID: 0000-0001-9931-9780

DOI: 10.32702/2306-6792.2020.12.66

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТ ІНФОРМАЦІЇ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВ

L. Bekhter,
PhD in Economics, Associate Professor, Department of Financial and Economic Security and Project Management, Zaporizhia National University, Zaporozhye

THREATS OF INFORMATION SECURITY AND PROTECTION OF INFORMATION AS A COMPONENT OF ECONOMIC SECURITY OF AGRICULTURAL ENTERPRISES

У статті розкривається сутність захисту інформації та інформаційної безпеки сільськогосподарських підприємств. Розглянуто один з найважливіших елементів, від стану якого залежить ступінь захисту інформації в системі сільськогосподарських відносин — інформаційну безпеку. Встановлено, що інформаційна безпека є однією з найголовніших складових економічної безпеки сільськогосподарських підприємств і займає одне із провідних місць досліджень вітчизняних науковців. Виокремлено проблемні питання щодо забезпечення інформаційної безпеки сільськогосподарських підприємств. Досліджуються питання забезпечення інформаційної безпеки підприємства. Розглянуто об'єкти, питання забезпечення та основні загрози інформаційної безпеки на підприємствах сільського господарства. Реалізація загроз є наслідком одного з таких дій і подій: розбовтування конфіденційної інформації, втрата конфіденційної інформації і недозволений доступ до інформації, що захищається. Запропоновано схеми з основними загрозами безпеки та подіями, що порушують інформаційну безпеку. Сформовано причини та умови, що створюють передумови для втрати комерційної інформації. Розглянуто певні вимоги до захисту інформації з позиції системного підходу. Запропоновано для різних, інформаційно не захищених, сільськогосподарських підприємств модель побудови системи захисту інформації, що описує сукупність об'єктивних зовнішніх і внутрішніх факторів і демонструє їх вплив на стан інформаційної безпеки. Розглянуто проблему класифікації інформаційних ресурсів. Значна частина інформаційних ресурсів у сучасному суспільстві є загальнодоступною, але при цьому існують джерела інформації, доступ до яких в силу тих чи інших причин обмежений. Складові частини, елементи, методи і засоби захисту інформаційних ресурсів у рамках будь-якої системи захисту повинні регулярно змінюватися з метою запобігання їх розкриття зацікавленим особам. Визначено економічну доцільність організації захисту інформації сільськогосподарських підприємств та в організаціях різних сфер господарської діяльності.

The article reveals the essence of information protection and information security of agricultural enterprises. One of the most important elements on the state of which the degree of information protection in the system of agricultural relations depends is considered — information security. It is established that information security is one of the most important components of economic security of agricultural enterprises and occupies one of the leading research sites of domestic scientists. Problematic issues related to information security of agricultural enterprises are highlighted. Issues of information security of the enterprise are investigated. The objects, issues of provision and the main threats to information security in agricultural enterprises are considered. The implementation of threats is the result of one of the following actions and events: disclosure of confidential information, loss of confidential information and unauthorized access to protected information. Schemes with the main security threats and events that violate information security are proposed. The reasons and conditions that create the preconditions for the loss of commercial information are formed. Certain requirements for information protection from the standpoint of a systems approach are considered. A model of information protection system construction has been proposed for various agricultural enterprises, which are not protected by information, which describes a set of objective external and internal factors and demonstrates their impact on the state of information security. The problem of classification of information resources is considered. Much of the information resources in modern society are publicly available, but there are sources of information, access to which for one reason or another is limited. The components, elements, methods and means of protection of information resources

Передплатний індекс 21847

within any security system must be changed regularly in order to prevent their disclosure to interested parties. The economic expediency of the organization of information protection of agricultural enterprises and in organizations of different spheres of economic activity is determined.

Ключові слова: інформаційна безпека, недозволений доступ, економічна безпека, захист інформації, сільськогосподарські підприємства, загрози інформаційної безпеки.

Key words: information security, unauthorized access, economic security, information protection, agricultural enterprises, information security threats.

ПОСТАНОВКА ПРОБЛЕМИ

На сьогодні інформаційні ресурси мають істотне значення в розвитку науки, техніці, виробництва, сфери послуг та інших галузевих складових. Значна їх частина в сучасному суспільстві є загальнодоступною, але водночас є джерела інформації, доступ до яких через ті чи інші причини обмежений. Таким чином, виникає проблема класифікації інформаційних ресурсів, обмеження доступу до деякої частини з них, визначення економічної доцільності організації захисту інформації на підприємствах, а саме: сільськогосподарських і в організаціях різних сфер господарської діяльності.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Не повний аналіз загроз і подій, що порушують інформаційну безпеку сільськогосподарських підприємств, не сформульовані достатні вимоги до захисту інформації.

Проблемні дослідження інформаційної складової економічної безпеки розглядали Г.А. Андрощук [1], І.А. Бланк [2], Н.В. Ващенко, Л.І. Донець [3], А.І. Захаров [4], С.А. Єрохін [5], В.П. Пономарьов [6] та ін. У цих роботах вивчається поняття економічної безпеки сільськогосподарських підприємств, розглядаються складові економічної безпеки, а саме інформаційна.

МЕТА СТАТТІ

Метою статті є дослідження загроз інформаційної безпеки і захист інформації як складової економічної безпеки сільськогосподарських підприємств.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Інформаційна безпека з точки зору економічної безпеки є станом захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, яке забезпечує збереження основних властивостей інформації та досягнення соціально-економічних цілей створення організації.

Інформаційна безпека — неможливість нанесення шкоди властивостям об'єкта безпеки, обумовлюється інформацією і інформаційною інфраструктурою (захищеність від загроз).

Інформаційна загроза має місце тоді, коли величина і ймовірність можливої інформаційної шкоди більші певного значення, що вимагає вживання заходів щодо його запобігання, захисту об'єкта безпеки.

Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів. Загрози схоронності, цілісності і конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик утворення каналу несанкціонованого отримання (добування) кимось цінної інформації і документів. Цей канал представляє собою сукупність незахищених або слабо захищених напрямів можливої втрати інформаційних ресурсів обмеженого доступу, які зловмисник використовує для отримання необхідних відомостей. Функціонування каналу несанкціонованого доступу до інформації обов'язково тягне за собою втрату інформації, зникнення носія інформації.

Забезпечення інформаційної безпеки має починатися з виявлення суб'єктів відносин, пов'язаних з використанням інформаційних систем. Спектр їхніх інтересів може бути розділений на наступні основні категорії: доступність, цілісність, конфіденційність.

Виходячи з вищевикладеного, в найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість нанесення шкоди властивостям об'єкта безпеки, обумовлена інформацією і інформаційною інфраструктурою.

До об'єктів інформаційної безпеки сільськогосподарських підприємств відносять:

— інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, та конфіденційну інформацію, представлену у вигляді інформаційних масивів і баз даних;

— засоби і системи інформатизації — засоби обчислювальної та організаційної техніки,

Передплатний індекс 21847

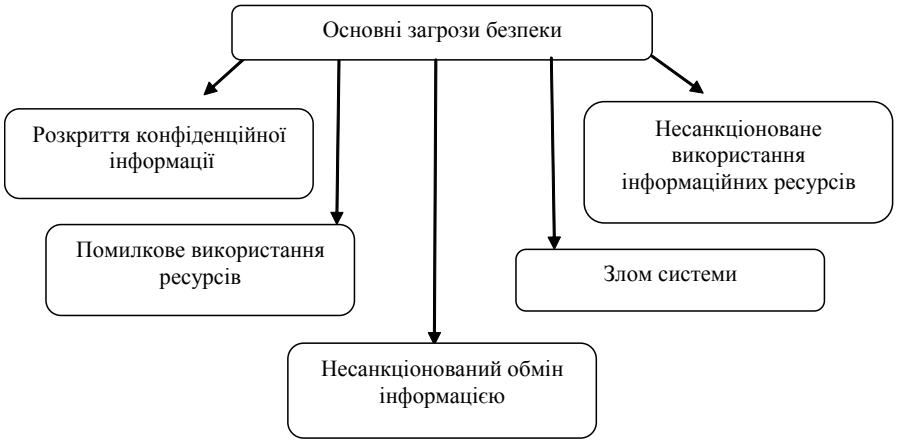

Рис. 1. Основні загрози інформаційної безпеки сільськогосподарських підприємств

мережі та системи, загальносистемне і прикладне програмне забезпечення, автоматизовані системи управління в організаціях, системи зв'язку і передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації.

Зловмисник може ознайомитися з конфіденційною інформацією, модифікувати її або навіть знищити, а також обмежити або блокувати доступ легального користувача до інформації. Водночас зловмисником може бути як співробітник організації, так і стороння особа.

Розглянемо основні загрози інформаційної безпеки.

Засобами реалізації загрози розкриття конфіденційної інформації можуть бути несанкціонований доступ до баз даних, прослуховування каналів і т.д. Реалізація загроз є наслідком однієї з таких дій і подій: розбовтування конфіденційної інформації, втрата конфіденційної інформації і недозволений доступ до інформації, що захищається. У разі розбовтування або втрати відбувається порушення конфіденційності інформації з обмеженим доступом (рис. 2).

Недозволений доступ — це найбільш поширений вид інформаційних загроз, що полягає в отриманні користувачем доступу до об'єкта, на який у нього немає дозволу відповідно до прийнятої в організації політикою інформаційної безпеки. За характером впливу недозволений доступ є активним впливом, що використовує помилки системи. Недозволеному доступу може бути підданий будь-який об'єкт системи. Водночас недозволений доступ, може бути досягнутий як стандартними, так і спеціально розробленими програмними засобами. Втрата конфіденційної інформації може привести до значного матеріального і морального збитку, як для організації, де функціонує інформаційна система, так і для її користувачів. Досить велика частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникає через елементарних недоробок керівників організацій, підприємств та їх співробітників.

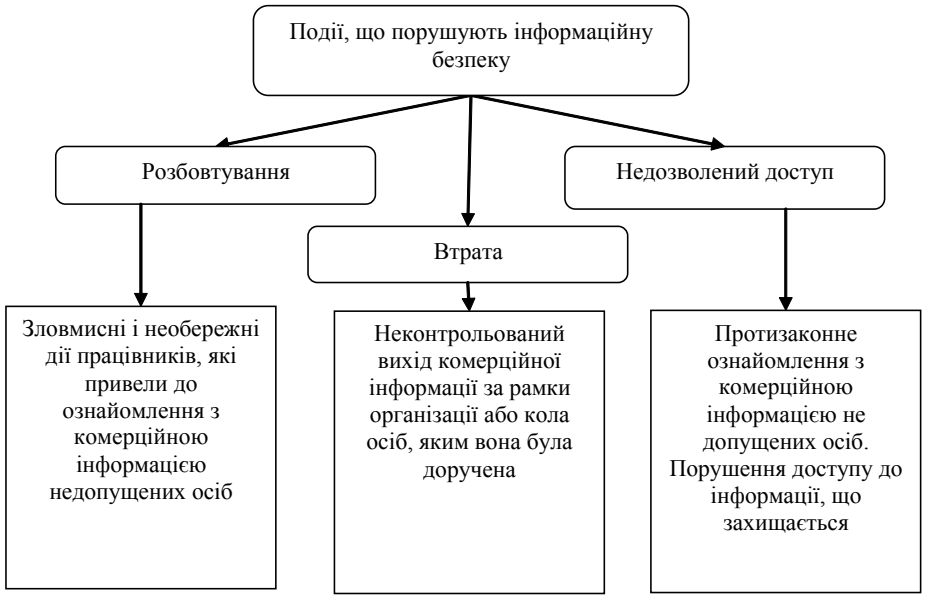

Рис. 2. Події, що порушують інформаційну безпеку сільськогосподарських підприємств

До причин і умов, що створюють передумови для втрати, можуть належати:

— недостатнє знання працівниками підприємств правил захисту конфіденційної інформації та нерозуміння необхідності їх ретельного дотримання;

— використання не атестованих технічних засобів обробки конфіденційної інформації;

— слабкий контроль над дотриманням правил захисту інформації правовими організаційними та інженерно-технічними заходами та ін. Помилкове

Передплатний індекс 21847

використання інформаційних ресурсів, будучи санкціонованими, тим не менш, може привести до руйнування, розкриття або компрометації вказаних ресурсів.

Значна загроза найчастіше є наслідком помилок в програмному забезпеченні автоматизованої інформаційної системи.

Захист інформації — комплекс заходів, спрямованих на забезпечення найважливіших аспектів інформаційної безпеки: цілісності, доступності і, якщо потрібно, конфіденційності інформації та ресурсів, що використовуються для введення, зберігання, обробки і передачі даних.

Загальні цілі захисту інформації — це запобігання розголошенню, втрати, несанкціонованого доступу, збереження цілісності, повноти, достовірності, дотримання конфіденційності, доступності, авторських прав.

Система захисту інформації являє собою організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

З позицій системного підходу до захисту інформації висуваються певні вимоги:

— забезпечення інформаційної безпеки не може бути одноразовим актом; це безперервний процес, що полягає в обгрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення та розвитку системи захисту, безперервному контролі її стану, виявлення її вузьких і слабких місць і протиправних дій;

— планування інформаційної безпеки здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції;

— захисту підлягають конкретні дані, об'єктивно що підлягають охороні, втрата яких може заподіяти організації певної шкоди;

— методи і засоби захисту повинні надійно перекривати можливі шляхи неправомірного доступу до секретів, що знаходяться під охороною;

— ефективність захисту інформації означає, що витрати на її здійснення не повинні бути більше можливих втрат від реалізації інформаційних загроз;

— чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;

— надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;

— зведення до мінімуму числа загальних для декількох користувачів засобів захисту;

— облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;

— забезпечення ступеня конфіденційної інформації;

— забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу. Система захисту інформації, як будь-яка система, повинна мати певні види власного забезпечення, спираючись на які вона буде виконувати свою цільову функцію.

З огляду на це система захисту інформації може мати:

— правове забезпечення (нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери дії);

— організаційне забезпечення (реалізація захисту інформації здійснюється певними структурними одиницями, а саме: служба безпеки, служба режиму, служба захисту інформації технічними засобами та ін.);

— апаратне забезпечення (використання технічних засобів, як для захисту інформації, так і для забезпечення діяльності власне системи захисту інформації);

— інформаційне забезпечення (документування відомостей, куди входять показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;

— програмне забезпечення (антивірусні програми, що реалізують контрольні функції при вирішенні облікових, статистичних, фінансових, кредитних та інших завдань;

— математичне забезпечення (використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон і норм необхідного захисту);

— нормативно-методичне забезпечення (норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації;

— ергономічне забезпечення. Сукупність засобів, що забезпечують зручності роботи, користувачів апаратних засобів захисту інформації.

У зв'язку з розкриттям проблематики інформаційної безпеки, з'являється очевидна необхідність побудови моделі системи захисту інформації, яка розглянута на рисунку 3.

Представлена модель описує сукупність об'єктивних зовнішніх і внутрішніх факторів і демонструє їх вплив на стан інформаційної безпеки на об'єкті та на збереження матеріальних або інформаційних ресурсів.

Передплатний індекс 21847

ВИСНОВКИ

Таким чином, значна частина інформаційних ресурсів у сучасному суспільстві є загальнодоступною, але при цьому існують джерела інформації, доступ до яких в силу тих чи інших причин обмежений. У статті розглянуто проблему класифікації інформаційних ресурсів, визначено економічну доцільність організації захисту інформації сільськогосподарських підприємств та в організаціях різних сфер господарської діяльності. Здійснено теоретичний аналіз загроз і подій, що порушують інформаційну безпеку, сформульовані в статті достатні вимоги до захисту інформації та побудовано модель системи захисту інформації для підприємств сільського господарства. Складові частини, елементи, методи і засоби захисту інформаційних ресурсів у рамках будь-якої системи захисту повинні регулярно змінюватися з метою запобігання їх розкриття зацікавленим особам.

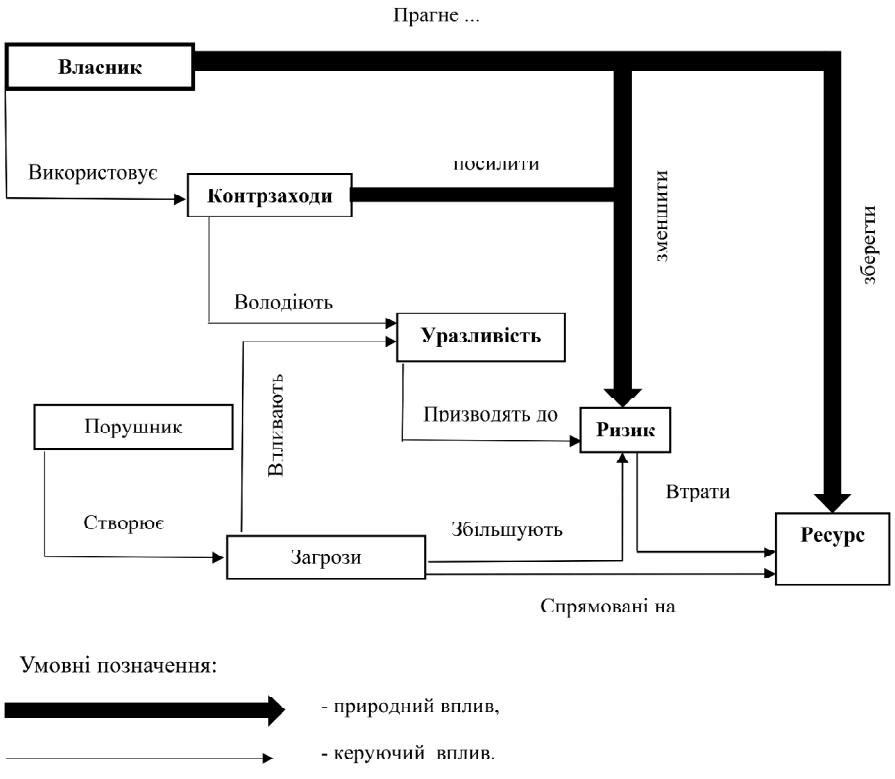

Рис. 3. Модель побудови системи захисту інформації сільськогосподарських підприємств

Література:

1. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны: учеб. пос. Киев: Дім "Ін Юре", 2000. 398 с.

2. Бланк И.А. Управление финансовой безопасностью предприятия: учеб. пос. Киев: Эльга, Ника-центр, 2004. 784 с.

3. Донець Л.І. Економічна безпека підприємства: навч. посіб. Київ: Центр учбової літератури, 2008. 240 с.

4. Захаров О.І. Організація та управління економічною безпекою суб'єктів господарської діяльності: навч. посіб. Київ: КНТ, 2008. 257 с.

5. Єрохін С.А. Структурна трансформація національної економіки (теоретико-методологічний аспект): монографія. Київ: "Світ знань", 2002. 528 с.

6. Пономарьов В.П. Формування механізму забезпечення економічної безпеки підприємства: автореф. дис. ... канд. екон. наук: 08.06.01. Луганськ, 2000. 21 с.

References:

1. Androshchuk, H. A. (2000), Jekonomycheskaia bezopasnost predpryiatyia: zashchyta kommercheskoi tainy [Economic salus coeptis: kommercheskoy tutela arcana], Dim "In Yure", Kyiv, Ukraine.

2. Blank, Y. A. (2004), Upravlenye fynansovoi bezopasnostiu predpryiatyia [Omnium fynansovoy bezopasnostyu Enterprise Management], "Jelha, Nika Centrum", Kyiv, Ukraine.

3. Donets, L. I. (2008), Ekonomichna bezpeka pidpryiemstva [Economic comitatu securitas], Tsentr uchbovoi literatury, Kyiv, Ukraine.

4. Zakharov, O. I. (2008), Orhanizatsiia ta upravlinnia ekonomichnoiu bezpekoiu subiektiv hospodarskoi diialnosti [Economic ordine et administratione rerum securitate negotium], KNT, Kyiv, Ukraine.

5. Ierokhin, S. A. (2002), Strukturna transformatsiia natsionalnoi ekonomiky (teoretyko-metodolohichnyi aspekt) [Structural mutatio in nationalis oeconomia (theoretical et methodo propter speciem)], "Svit znan", Kyiv, Ukraine.

6. Ponomarov, V. P. (2000), "Formation of the mechanism of ensuring economic security of the enterprise", Ph.D. Thesis, Global economy, Luhansk, Ukraine.

Стаття надійшла до редакції 16.06.2020 р.