УДК 338

ІНФОРМАЦІЙНА СКЛАДОВА У СТРУКТУРІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

© 2017 **БОРЗЕНКОВА О. Д., ШРАМКО О. О.**

УДК 338

Борзенкова О. Д., Шрамко О. О. Інформаційна складова у структурі економічної безпеки підприємства

Формування економічної безпеки підприємства полягає в розробці та впровадженні системи управління та комплексу заходів, спрямованих на виробничу та невиробничу сфери з метою забезпечення ефективної господарської діяльності, мінімізації факторів впливу та загроз в умовах мінливого зовнішнього середовища. У статті визначено сутність та роль інформаційної складової, що полягає в захищеності інформаційного середовища, діяльності щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію і т. ін. Інформаційна безпека підприємства досягається: заходами правового забезпечення на рівні держави та підприємства; організаційного забезпечення (тобто регулювання інформаційного потоку на підприємстві); програмно-технічного забезпечення (як програмного та апаратного облаштування з метою запобігання незаконному витоку інформації).

Ключові слова: *інформація, інформаційні технології, конфіденційна інформація, комерційна таємниця, інформаційне середовище, економічна безпека підприємства.*

Рис.: *3.* ***Бібл.:*** *13.*

Борзенкова Ольга Дмитрівна *– кандидат економічних наук, доцент кафедри фінансів, банківської справи та страхування, Одеський торговельно-економічний інститут Київського національного торговельно-економічного університету (вул. 25 Чапаївської дивізії, 6, Одеса, 65070, Україна)*

E-mail: *Ob-2010@rambler.ru*

Шрамко Олена Олександрівна *– старший викладач кафедри вищої математики та інформаційних технологій, Одеський торговельно-економічний інститут Київського національного торговельно-економічного університету (вул. 25 Чапаївської дивізії, 6, Одеса, 65070, Україна)*

E-mail: *Eschramko@yandex.ru*

УДК 338

Борзенкова О. Д., Шрамко Е. А. Информационная составляющая в структуре экономической безопасности предприятия

Формирование экономической безопасности предприятия заключается в разработке и внедрении системы управления и комплекса мер, направленных на производственную и непроизводственную сферы с целью обеспечения эффективной хозяйственной деятельности, минимизации факторов влияния и угроз в условиях меняющейся внешней среды. В статье определена сущность и роль информационной составляющей, которая заключается в защищенности информационной среды, деятельности по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию и т. п. Информационная безопасность предприятия обеспечивается: мерами правового обеспечения на уровне государства и предприятия; организационного обеспечения (то есть регулирования информационного потока на предприятии); программно-технического обеспечения (как программного и аппаратного обеспечения с целью предотвращения незаконной утечки информации).

Ключевые слова: *информация, информационные технологии, конфиденциальная информация, коммерческая тайна, информационная среда, экономическая безопасность предприятия.*

Рис.: *3.* ***Библ.:*** *13.*

Борзенкова Ольга Дмитриевна *– кандидат экономических наук, доцент кафедры финансов, банковского дела и страхования, Одесский торгово-экономический институт Киевского национального торгово-экономического университета (ул. 25 Чапаевской дивизии, 6, Одесса, 65070, Украина)*

E-mail: *Ob-2010@rambler.ru*

Шрамко Елена Александровна *– старший преподаватель кафедры высшей математики и информационных технологий, Одесский торгово-экономический институт Киевского национального торгово-экономического университета (ул. 25 Чапаевской дивизии, 6, Одесса, 65070, Украина)*

E-mail: *Eschramko@yandex.ru*

UDC 338

Borzenkova O. D., Shramko O. O. The Information Component in the Structure of the Enterprise's Economic Security

Developing the enterprise's economic security consists in elaboration and implementation of a management system and a complex of activities aimed at the production and nonproduction spheres, with a view to ensuring an efficient economic performance, minimizing the factors of influence and threats in the changing external environment. The article defines the nature and role of the information component which consists of protection of the information environment, activities to prevent leakages of protected information, unauthorized and unintentional impacts on information, etc. The information security of enterprise is ensured by: legal measures at the level of the State and the level of enterprise; organizational support (i.e. regulation of the information flow at the enterprise); firmware (both software and hardware support to prevent illegal leakages of information).

Keywords: *information, information technology, confidential information, commercial confidentiality, information environment, economic security of enterprise.*

Fig.: *3.* ***Bibl.:*** *13.*

Borzenkova Olga D. *– PhD (Economics), Associate Professor of the Department of Finance, Banking and Insurance, Odesa Institute of Trade and Economy of Kyiv National University of Trade and Economy (6 25 Chapaivskoi Dyvizii Str., Odesa, 65070, Ukraine)*

E-mail: *Ob-2010@rambler.ru*

Shramko Olena O. *– Senior Lecturer of the Department of Mathematics and Information Technologies, Odesa Institute of Trade and Economy of Kyiv National University of Trade and Economy (6 25 Chapaivskoi Dyvizii Str., Odesa, 65070, Ukraine)*

E-mail: *Eschramko@yandex.ru*

Формування економічної безпеки підприємства передбачає існування гнучкої системи управління, здатної оперативно виявляти зміни в зовнішньому середовищі та реагувати на них, уможливлюючи функціонування підприємства у будь-яких умовах та надавати можливість адаптації до таких змін. Відомо, що до одного з найбільш впливових елементів економічної безпеки підприємства належить інформаційна складова як пріоритетний фактор виробництва в умовах інформаційного суспільства.

Сутність поняття економічної безпеки підприємства та її основні функціональні складові досліджува-

ла С. А. Левицька [7; 8]. Структуру економічної безпеки підприємства в умовах кризи вивчали Ю. О. Ярова, Л. П. Артеменко [13]. Визначення реалій та загроз щодо інформаційної безпеки підприємства здійснили В. М. Абакумов [1], Г. Я. Аніловська [2], О. В. Діброва [4], С. В. Легомінова [9], С. В. Северина [11], Л. Г. Чистоклетов [12]. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві визначала А. Ю. Нашинець-Наумова [10]. Програмно-технічне забезпечення захисту інформації вивчали: Т. І. Зоріна – в частині системи виявлення та запобігання атакам у комп'ютерних мережах [5] та О. П. Козевич – у напрямі контентної фільтрація як технології комплексного контролю Інтернет-ресурсів [6].

Мета статті полягає в ідентифікації сутності економічної безпеки підприємства та її основних складових, факторів впливу на формування та можливих загроз, визначенні місця та ролі інформаційної складової у структурі економічної безпеки.

Діяльність підприємства охоплює різні напрями і повинна розглядатись у взаємозв'язку виробничої та невиробничої сфер, оскільки кожна з них створена з метою забезпечення ефективної діяльності. Таким чином, формування економічної безпеки підприємства включає комплекс заходів, що спрямовані на захист кожної зі складових.

Як зазначає С. А. Левицька, поняття «економічна безпека підприємств» означає комплексну характеристику, під якою розуміють рівень захищеності всіх видів потенціалу (науково-технічного, технологічного, виробничого, кадрового) підприємства від внутрішніх та зовнішніх загроз, що забезпечує стабільний розвиток та ефективне функціонування підприємства, а забезпечення економічної безпеки є однією з головних складових успішного ведення підприємницької діяльності [8, с. 53].

У сучасному інформаційному суспільстві інформація є пріоритетним фактором виробництва, що в сукупності з оперативним прийняттям управлінських рішень здатні суттєво вплинути на господарську діяльність підприємства. Відсутність необхідної інформації про ринок для суб'єкта господарювання або її невідповідність основним якісним критеріям: повнота, достовірність, вчасність здатні повністю припинити діяльність такого підприємства. Крім того, втрата чи розповсюдження інформації може суттєво вплинути на діяльність суб'єкта господарювання, його фінансові показники та результати діяльності, навіть незалежно від наявних активів. Таким чином, інформаційна складова відіграє одну з головних ролей у забезпеченні економічної безпеки підприємства.

Досліджуючи інформаційну безпеку та методи захисту інформації, С. В. Северина зазначає, що в сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку. Заходи щодо забезпечення інформаційної безпеки є завданням для бізнесу та економічної системи задля розвитку, посилення конкурентних позицій на ринку [11, с. 160].

Вивчаючи основні положення управління інформаційною безпекою в сучасних умовах, О. В. Діброва зазначає, що при неналежному рівні управління інформаційною безпекою всі заходи щодо створення чи здобуття інформації будуть зведені нанівець, оскільки вона з легкістю може стати відомою зловмисникам, що може стати причиною виникнення конфлікту, збитків, небезпеки [4, с. 7–8].

Таким чином, головні складові економічної безпеки підприємства, сутність та завдання інформаційної безпеки підприємства наведено на *рис. 1*.

Отже, однією з найважливіших складових у структурі економічної безпеки підприємства є інформаційна частина, що передбачає створення єдиної системи даних щодо діяльності підприємства, а основне завдання для керівництва полягає в розробці заходів щодо її забезпечення.

Досліджуючи інформаційну безпеку підприємства як об'єкт адміністративно-правової охорони, В. М. Абакумов зазначає, що саме поняття «інформаційна безпека підприємництва» означає сукупність заходів, визначених на рівні нормативно-правових актів, що регламентують підприємницьку діяльність і визначають особливості захисту інформації суб'єктами господарювання в Україні, та внутрішніх правил конкретного підприємства, спрямованих на захист інформаційного ресурсу підприємств, нейтралізацію та ліквідацію загроз ефективному функціонуванню інформаційної системи суб'єкта господарської діяльності зокрема та діяльності цього суб'єкта в цілому [1, с. 13].

Складові інформаційної безпеки підприємства систематизовано на *рис. 2*.

Таким чином, інформаційна безпека підприємства забезпечується заходами *правового забезпечення* щодо державної політики в напрямах правового поля, прав та обов'язків суб'єктів, зокрема інформаційного права; *організаційного забезпечення*, що визначає правила та заходи надходження та обробки інформації на підприємстві; *програмно-технічного забезпечення*, що уможливлює захист інформації за допомогою технічних засобів, а також надає можливість прийняття технічних рішень.

Варто зазначити, що правове забезпечення формується на рівні держави, а на рівні підприємства це передбачає розробку та впровадження положення про інформаційну безпеку за напрямами: визначення об'єктів, що становлять комерційну таємницю, заходи щодо збереження інформації, відповідальність за розголошення і т. д.

Для функціонування організаційного забезпечення важливу роль відіграє система бухгалтерського обліку, що реєструє факти господарського життя. Взаємозв'язок організаційних заходів та програмно-технічного забезпечення виявляться в автоматизації відповідних процесів.

Як зазначає Г. Я. Аніловська, наявні системи автоматизації обліку реалізують такі способи вводу первинної інформації в систему: через журнал обліку господарських операцій; з використанням типових операцій, че-

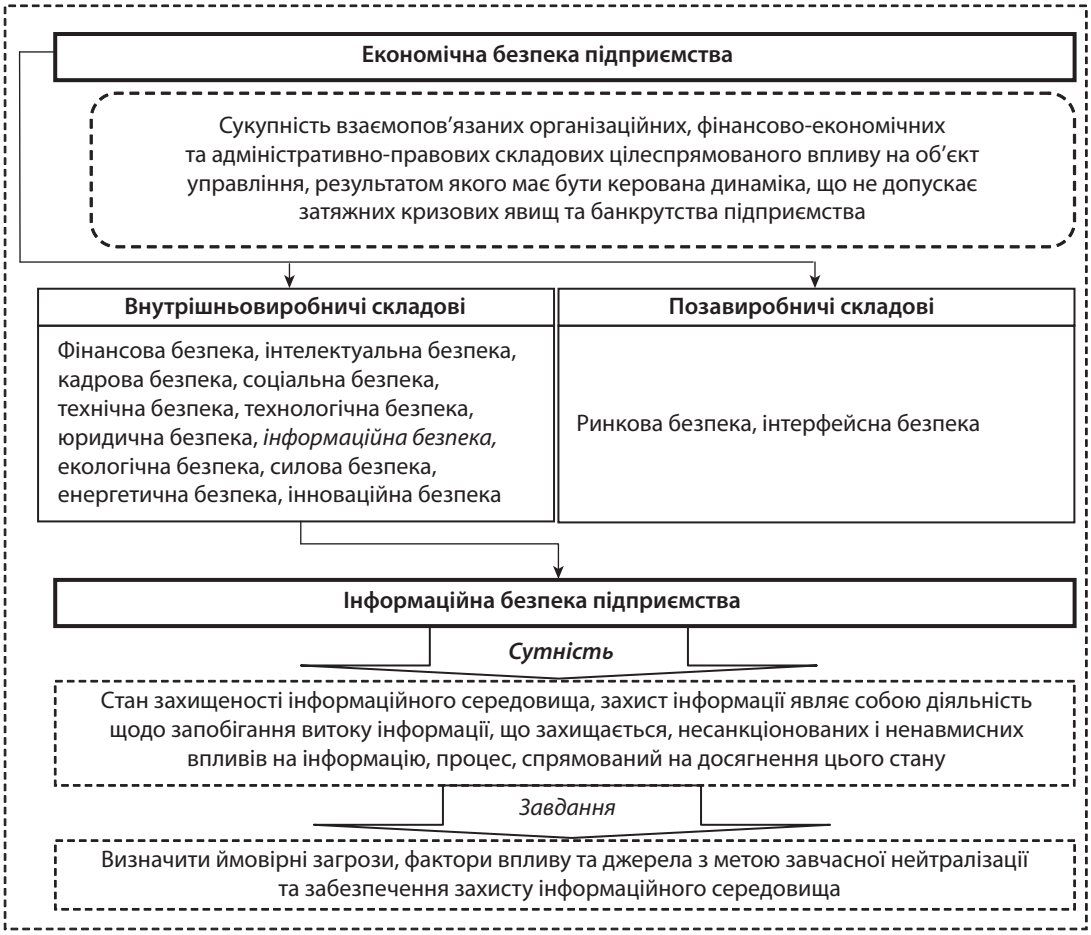

Рис. 1. Складові економічної безпеки підприємства

Джерело: складено за [7, с. 385; 13, с. 260].

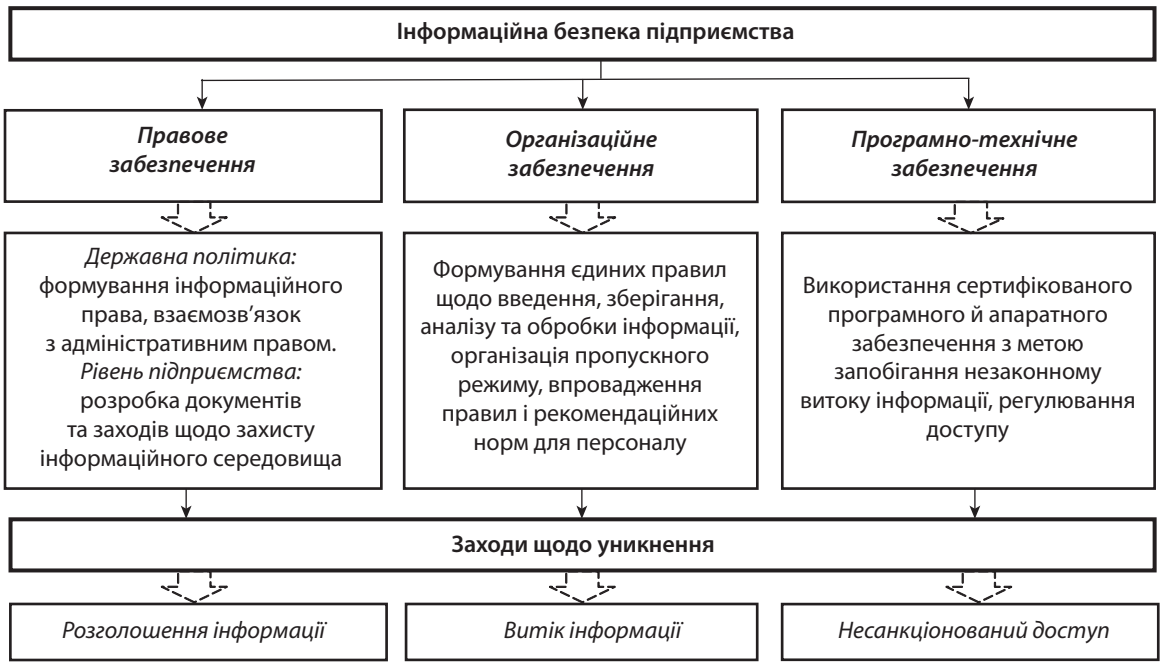

Рис. 2. Напрями забезпечення інформаційної безпеки підприємства

Джерело: складено за [1, с. 13–14;12, с. 224–226].

рез шаблон електронного документа. На думку автора, обов'язковим є забезпечення можливості ідентифікації точки введення та проходження документа в процесі оброблення від одного виконавця до іншого, відповідно до технологічної схеми ведення обліку, забезпечення ведення протоколу парольних входів у систему з кожного робочого місця і виконуваних дій, що надасть можливість контролювати дії користувачів системи та уникати можливих зловживань [2, с. 272].

Однак використання програмно-технічного забезпечення не гарантує абсолютного захисту даних. Так, захист конфіденційної інформації на підприємстві стає все більш актуальною проблемою з огляду на те, що серйозні негативні наслідки виникають у компаніях ІТ-сфери при втраті інформації (баз даних), результатів аналітичних досліджень, початкових кодів, програмних продуктів, персональних даних клієнтів, без яких подальше продовження бізнесу стає проблемним [10, с. 118].

Як зазначає О. П. Козевич, сучасна ІТ-структура піддається великій кількості атак, найбільш актуальними з яких є:

- фішінг (*fishing*) – способи перехоплення паролей, номерів кредитних карт і т. п. за допомогою технік соціальної інженерії;
- Spyware & Malware – засоби перехоплення даних і встановлення контролю над комп'ютером;
- віруси та інші шкідливі коди;
- SPAM/SPIM – небажані повідомлення, що засмічують електронну пошту;
- витік бізнес-інформації, що може нанести компанії невиправну шкоду;
- загроза судового переслідування, пов'язана з неправомірним використанням інформації, яка захищена авторським правом [6, с. 134–135].

Так, жертвами хакерів за підсумками 2015 р. стали 594 мільйони осіб по всьому світу. Відповідно до звіту з кібербезпеки від американської антивірусної компанії Symantec Corporation споживачі електронних сервісів по всьому світу втратили від скоєних у 2015 р. кіберзлочинів 158 мільярдів доларів. У тому числі у США втрати населення від кіберзлочинів склали 30 млрд дол. [3].

Це свідчить про необхідність посилення захисту інформації, постійного оновлення програмного забезпечення відповідно до розвитку технологій. Системи інформаційного захисту підприємства розвиваються паралельно з розвитком програм, які мають негативний вплив. Основні інструменти щодо забезпечення інформаційної безпеки підприємства систематизовано на *рис. 3*.

Таким чином, найбільш поширеними є засоби ідентифікації та автентифікації користувачів, шифрування інформації та засоби антивірусного захисту. Використання таких програм надає можливість контролю за діями користувачів у інформаційній системі, у випадку копіювання даних не дозволить іншим користувачам зрозуміти отриману інформацію за рахунок застосування шифру, а засоби антивірусного захисту забезпечать нейтралізацію шкідливих програм.

Вивчаючи теоретичні засади інформаційної безпеки підприємства, С. В. Легомінова також зазначає, що особливе місце займають криптографічні методи захисту інформації. Інтерес комерційних структур до них значно зріс у зв'язку зі зменшенням вартості перехоплення інформації, що передається електронною поштою чи функціонує в системі електронних платежів. Найпоширенішими вважаються методи кодування та шифрування інформації, методи розділення та стиснення даних. У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням [9, с. 89].

Поширеним інструментом формування інформаційної безпеки також є системи виявлення вразливості мереж і аналізатори мережевих атак, впровадження яких для підприємств надає значні переваги, зокрема:

- розпізнавання відомих і, по можливості, невідомих атак, попередження про них, статистичний аналіз шаблонів аномальних дій;
- моніторинг і аналіз користувальницької, мережевої та системної активності, контроль цілісності файлів та інших ресурсів інформаційної системи, аудит системної конфігурації та виявлення вразливості;
- зниження навантаження на персонал, що відповідає за інформаційну безпеку, від поточних рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами інформаційних систем, надання можливості управління засобами захисту експертам у сфері безпеки [5, с. 48].

Таким чином, враховуючи різноманіття існуючих інструментів щодо захисту інформації, кожне підприємство повинно самостійно визначати необхідність встановлення відповідних програм, залежно від потреб. Ураховувати варто масштаби діяльності підприємства, галузь, унікальність продукту та технології, ринок, фінансові ресурси підприємства та ін.

Зокрема, для суб'єктів господарювання, які функціонують на ринку недобросовісної конкуренції, застосування інструментів інформаційного захисту є обов'язковим. Підприємствам, що розробляють унікальний продукт чи послуги, також варто посилити інформаційний захист, оскільки розголошення такої інформації призведе до аналогів і вплине на ринкову стійкість підприємства. Крім того, варто визначити, в який спосіб забезпечується інформаційна безпека на підприємстві – власними силами чи за допомогою залучених організацій, чи враховується вартість систем, які впроваджуються в дію.

ВИСНОВКИ

Формування економічної безпеки підприємства полягає в розробці та впровадженні системи управління та комплексу заходів, спрямованих на виробничу та невиробничу сфери з метою забезпечення ефективної господарської діяльності, мінімізації факторів впливу та загроз в умовах мінливого зовнішнього середовища. Підприємство, яке планує посилити конкурентні позиції на ринку, покращити показники діяльності, повинно

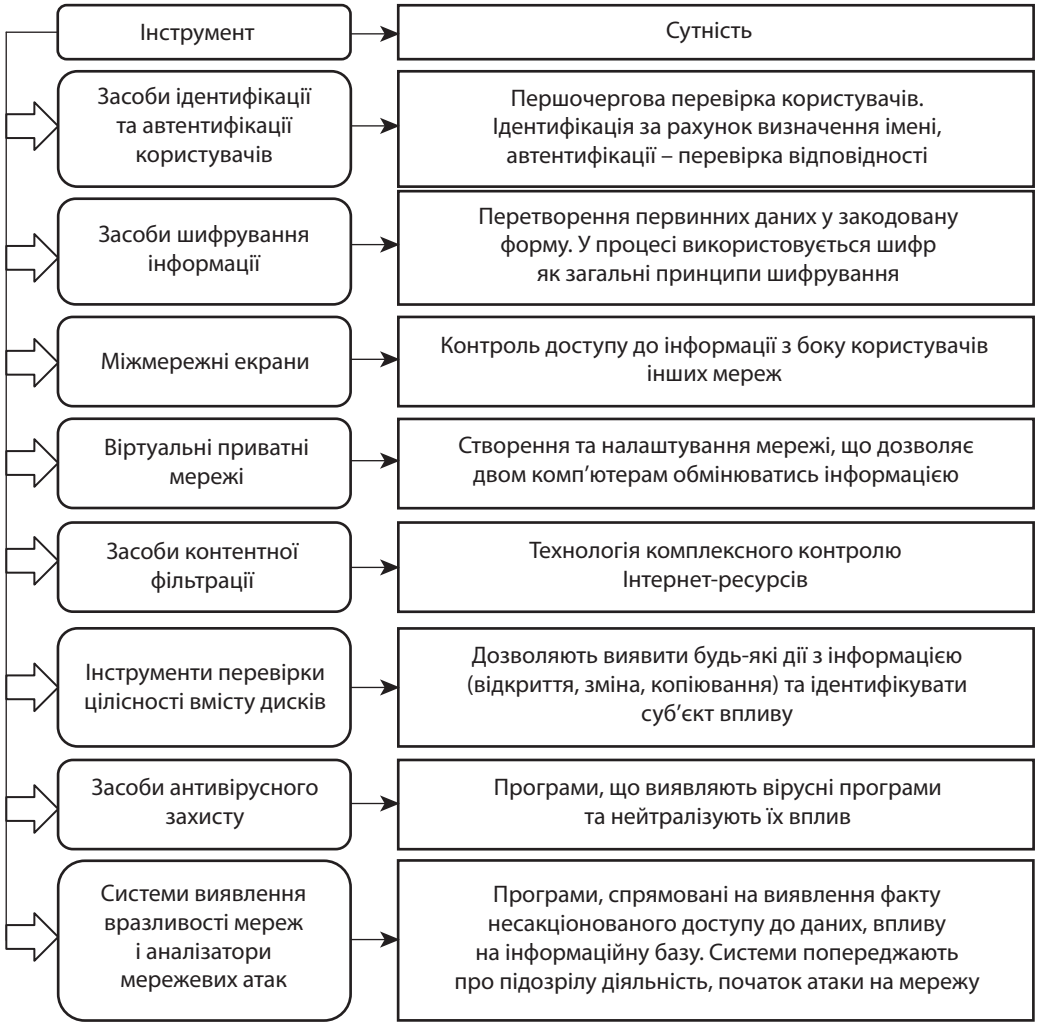

Рис. 3. Інструменти забезпечення інформаційної безпеки підприємства

Джерело: систематизовано та доповнено за [9, с. 89].

оперативно реагувати на зміни та мати гнучку систему управління. Наявність якісної інформації та прийняття на її основі рішень надають таку можливість, що визначає інформаційну складову економічної безпеки підприємства як пріоритетну.

Визначено, що інформаційна безпека підприємства забезпечується заходами правового забезпечення на рівні держави та підприємства, організаційного забезпечення, тобто регулювання інформаційного потоку на підприємстві, програмно-технічного забезпечення як програмного та апаратного облаштування з метою запобігання незаконному витоку інформації. Однак впровадження інформаційних технологій як сприяє захисту інформації, так і вимагає посилення організаційних заходів, збільшення витрат, залучення відповідних спеціалістів, що свідчить про взаємозв'язок всіх процесів на підприємстві як єдиної системи, що в цілому передбачає забезпечення як інформаційної, так і економічної безпеки підприємства.

Розробка та впровадження інформаційної безпеки за допомогою програмно-технічного забезпечення повинна враховувати вартість програм і систем, необхідність залучення спеціалістів чи можливість створення служби інформаційної безпеки на підприємстві. Головними факторами при визначенні необхідності впровадження інструментів інформаційного захисту є масштаби діяльності, унікальність продукції чи послуги, ринок та наявні фінансові ресурси підприємства, призначені для даних цілей. ■

ЛІТЕРАТУРА

1. Абакумов В. М. Інформаційна безпека підприємства як об'єкт адміністративно-правової охорони. *Форум права.* 2012. № 4. С. 10–16.

2. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник НЛТУ України*. 2008. Вип. 18.9. С. 270–273.

3. Втрати споживачів від кіберзлочинів склали 158 мільярдів доларів. URL: https://www.rbc.ua/ukr/lnews/poteri-potrebiteley-kiberprestupleniy-sostavili-1453718800.html

4. Діброва О. В. Огляд основних положень управління інформаційною безпекою в сучасних умовах. *Технології та дизайн*. 2014. № 4. С. 1–9.

5. Зоріна Т. І. Системи виявлення і запобігання атак в комп'ютерних мережах. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2013. № 15 (1). С. 48–52.

6. Козевич О. П. Контентна фільтрація – технологія комплексного контролю Інтернет-ресурсів. Основні підходи і проблеми. *Вісник Національного університету «Львівська по-*

літехніка». Сер.: Автоматика, вимірювання та керування. 2013. № 774. С. 134–141.

7. Левицька С. А. Основні функціональні складові економічної безпеки підприємства. *Молодий вчений*. Сер.: Економічні науки. 2016. № 10 (37). С. 385–388.

8. Левицька С. А. Теоретичний аналіз поняття економічної безпеки підприємств. *Науковий вісник Херсонського державного університету*. Сер.: Економічні науки. 2016. Вип. 19. Ч. 2. С. 52–53.

9. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. С. 87–92.

10. Нашинець-Наумова А. Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві. *Юридичний вісник. Повітряне і космічне право*. 2012. № 4. С. 118–122.

11. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету*. Сер.: Економічні науки. 2016. № 1. С. 155–161.

12. Чистоклетов Л. Г. Інформаційна безпека підприємства – як складова економічної безпеки: сучасні реалії та загрози. *Наукові записки Львівського університету бізнесу та права*. 2011. Вип. 7. С. 222–227.

13. Ярова Ю. О., Артеменко Л. П. Структура економічної безпеки підприємства в умовах кризи. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут»*. 2016. № 13. С. 257–263.

REFERENCES

Abakumov, V. M. "Informatsiina bezpeka pidpryiemstva yak obiekt administratyvno-pravovoi okhorony" [Information security of the enterprise as the object of administrative-legal protection]. *Forum prava*, no. 4 (2012): 10-16.

Anilovska, H. Ya. "Informatsiina bezpeka pidpryiemstva v umovakh vykorystannia suchasnykh informatsiinykh tekhnolohii" [Information security company in the terms of use of modern information technologies]. *Naukovyi visnyk NLTU Ukrainy*, no. 18.9 (2008): 270-273.

Chystokletov, L. H. "Informatsiina bezpeka pidpryiemstva - yak skladova ekonomichnoi bezpeky: suchasni realii ta zahrozy" [Information security company as a component of economic security: today's realities and threats]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava*, no. 7 (2011): 222-227.

Dibrova, O. V. "Ohliad osnovnykh polozhen upravlinnia informatsiinoiu bezpekoiu v suchasnykh umovakh" [An overview of the main provisions of information security management in modern conditions]. *Tekhnolohii ta dyzain*, no. 4 (2014): 1-9.

Kozevych, O. P. "Kontentna filtratsiia - tekhnolohiia kompleksnoho kontroliu Internet-resursiv. Osnovni pidkhody i problemy" [Content filtering technology integrated control of Internet resources. The main approaches and problems]. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika»*. Ser.: Avtomatyka, vymiriuvannia ta keruvannia, no. 774 (2013): 134-141.

Levytska, S. A. "Osnovni funktsionalni skladovi ekonomichnoi bezpeky pidpryiemstva" [The main functional components of economic security of enterprise]. *Molodyi vchenyi*. Ser.: Ekonomichni nauky, no. 10 (37) (2016): 385-388.

Levytska, S. A. "Teoretychnyi analiz poniattia ekonomichnoi bezpeky pidpryiemstv" [Theoretical analysis of the concept of economic security of enterprises]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Ekonomichni nauky*. Vol. 2, no. 19 (2016): 52-53.

Lehominova, S. V. "Teoretychni zasady informatsiinoi bezpeky pidpryiemstva" [Theoretical bases of information security of the enterprise]. *Ekonomika. Menedzhment. Biznes*, no. 3 (2015): 87-92.

Nashynets-Naumova, A. Yu. "Problemy pravovoho rehuliuvannia dostupu do konfidentsiinoi informatsii na pidpryiemstvi" [Problems of legal regulation of access to sensitive information in the enterprise]. *Yurydychnyi visnyk. Povitriane i kosmichne pravo*, no. 4 (2012): 118-122.

Severyna, S. V. "Informatsiina bezpeka ta metody zakhystu informatsii" [Information security and protection of information]. *Visnyk Zaporizkoho natsionalnoho universytetu*. Ser.: Ekonomichni nauky, no. 1 (2016): 155-161.

"Vtraty spozhyvachiv vid kiberzlochyniv sklaly 158 miliardiv dolariv" [Loss of consumers from cybercrime totalled 158 billion dollars]. https://www.rbc.ua/ukr/lnews/poteri-potrebiteley-kiber-prestupleniy-sostavili-1453718800.html

Yarova, Yu. O., and Artemenko, L. P. "Struktura ekonomichnoi bezpeky pidpryiemstva v umovakh kryzy" [The structure of economic security of enterprise in crisis conditions]. *Ekonomichnyi visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy «Kyivskyi politekhnichnyi instytut»*, no. 13 (2016): 257-263.

Zorina, T. I. "Systemy vyiavlennia i zapobihannia atak v kompiuternykh merezhakh" [Detection and prevention of attacks in computer networks]. *Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia*, no. 15 (1) (2013): 48-52.