УДК 004.056.5

В. Ю. Медвідь,
д. е. н., професор, професор кафедри менеджменту ім. І.А. Маркіної,
Полтавський державний аграрний університет,
ORCID ID: https://orcid.org/0000-0002-2257-6276
О. М. Правдивець,
к. військ. н., доцент, доцент кафедри фінансово-економічної безпеки Науково-навчального інституту менеджменту бізнесу, ВНЗ "Університет економіки та права "КРОК"
ORCID ID: https://orcid.org/0000-0001-5242-9683
Р. Ю. Кривчун,
здобувач вищої освіти спеціальності "Менеджмент",
Полтавський державний аграрний університет
ORCID ID: https://orcid.org/0000-0002-3671-0587

DOI: 10.32702/2306-6792.2023.1.24

ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

V. Medvid,
Doctor of Economic Sciences, Professor, Professor of the Department
of Management named after I.A. Markina, Poltava State Agrarian University
O. Pravdyvets,
PhD in Military Science, Associate Professor of the Department of Financial and Economic Security,
Research and Training Institute of Business Management, "KROK" University
R. Kryvchun,
Applicant for higher education specialty Management, Poltava State Agrarian University

FORMATION OF INFORMATION SECURITY MANAGEMENT SYSTEM AT ENTERPRISE: THEORETICAL AND METHODOLOGICAL PRINCIPLES

У статті визначено, що важливість цього напрямку дослідження полягає, перш за все, в обгрунтуванні необхідності формування комплексної системи діагностики рівня інформаційної безпеки та кількісної і якісної оцінки стану рівня інформаційної захищеності підприємства. Проаналізувавши визначення, сформовано поняття інформаційної безпеки, під яким мається на увазі рівень захищеності інформаційних джерел, що забезпечують формування суспільства і розвиток в інтересах держави, громадян, організації. Визначено, що модель системи інформаційної безпеки підприємства поєднує внутрішні та зовнішні фактори і те як вони впливають на загальний стан інформаційної безпеки підприємства та забезпечення безпеки ресурсів. Досліджено, що формування надійної системи інформаційної безпеки підприємства передбачає широкий спектр процедур, спрямованих на мінімізацію внутрішніх та зовнішніх загроз, які обмежені у часі та ресурсах.

Frequent changes in the economies of countries around the world constantly require changes in their security quality and its improvement. Monitoring innovations in terms of security or protecting the system from hacking is a priority task of those engaged in the organization of security systems at the enterprise.

Передплатний індекс 21847

A huge amount of information needs to be identified and managed for the safe operation of any enterprise. Safety-oriented activities are closely related to the risk management process. It is necessary to monitor an enterprise's internal information resources and carefully analyze external ones. Information is a set of certain data that describe the state of controlled and controlling subsystems and the external environment, the results and the subjects of the enterprise's management activity.

The article argues that the importance of this research goal is primarily related to substantiating the need to form a comprehensive system for diagnosing and quantitative and qualitative assessment of the enterprise's information security level. After analyzing the definition, the concept of information security was determined. It concerns the security level of information sources that ensure the formation and development of society with a focus on the interests of the state, citizens, and organizations. According to the study, the model of the information security management system of the enterprise combines internal and external factors and reflects their impact on the general state of the enterprise's information security and ensuring the security of its resources. The model assumes the presence of classic components to ensure the protection of the company's information infrastructure: subjects of information infrastructure management and subjects of information security management, objects, subjected to digital and information protection, as well as the management process itself, which involves the strategy, information security policy (informal), goals, methods, functions, measures, and tools. The research conclusions prove that the formation of a reliable information security system for the enterprise involves a wide range of procedures aimed at minimizing internal and external threats that are limited in time and resources.

Ключові слова: управління, підприємство, інформація, безпека, інформаційна безпека, кіберзлочинність, шпигунство.

Key words: management, enterprise, information, security, information security, cybercrime, espionage.

ПОСТАНОВКА ПРОБЛЕМИ

За рахунок масової інформатизації й комп'ютеризації товарного ринку підприємства мають доступ до будь-якої інформації, що спричиняє оптимізацію процесу виробництва, управління і збуту продукції. Проте, останнім часом випадки кіберзлочинності та електронного шахрайства стали частішими, що, відповідно, негативно відображаються на діяльності суб'єктів господарювання.

Часте застосування визначень: керування інформаційною безпекою, управління інформаційними ресурсами, кібератаки чітко демонструє той факт, що проблема інформаційної безпеки є невід'ємною частиною загальної системи організації управління. У наш час необхідно приділяти особливу увагу управлінню інформаційною безпекою, адже завдяки грамотному та якісному управлінню безпекою, інформаційна безпека та стійкість підприємства значно зросте.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблемі забезпечення інформаційної безпеки суб'єктів господарювання значну увагу приділено у працях таких науковців, як Голубєв В. [1], Дячков Д. [2], Залевська І. [3], Захаров Є. [4], Збожинський С. [5], Кавун С. [6], Калетнік В., Калетнік Н. [7], Кісілевич-Чорнойван О. [8], Лосєв І. [9], Маракова І., Сиропятов О. [10], Маркіна І. [11], Нестеренко О. [12], Степанов В. [13], Потапенко О. [14], Солодка О. [15], Федулова С. [16] та інших.

МЕТЕ СТАТТІ

Метою статті є обгрунтування теоретичних і методичних Засад формування системи управління інформаційною безпекою підприємства.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Швидкий темп зростання науково-технічного знання, широкий доступ до засобів роз-

Передплатний індекс 21847

робки програмного забезпечення та апаратного комп'ютерного забезпечення та можливостей застосування останнього є причинами високої вразливості підприємств до загроз різного характеру. Першоджерелом такої вразливості є неточності та недоліки існуючої політики проведення заходів інформаційної безпеки підприємств Відтак, безпечність функціонування суб'єктів господарювання в умовах трансформації бізнес-середовища, захист систем управління виробничими, управлінськими, технологічними процесами, захищеність об'єктів інформаційної інфраструктури визнаються актуальними завданнями, які потребують формування теоретичного базису безпекології в сфері інформаційної захисту та практичної його реалізації

Усі підприємства мають розуміти та планувати, як саме вони будуть йти до свого успіху, але на цьому шляху, вагомим елементом є його можливість забезпечити безпеку своєї конфіденційної інформації.

Часті зміни в економіках країн постійно змінюють та надають нові вимоги до якості безпеки. Слідкування за новинками в плані безпеки та зломів системи є пріоритетним завданням тих, хто займається організацією безпеки на підприємстві.

Мінімізація ризиків викрадення даних є основною причиною виникнення та створення інформаційної безпеки на підприємстві. Адже чим складніша система інформаційної безпеки на підприємстві, тим важче зловмисниками заволодіти конфіденційною інформацією. Чим дорожчим буде планування та організація зломів, фізичних викрадень або фізичного знищення даних, тим більше зловмисники будуть задумуватися про кінцевий результат своєї неправомірної діяльності і чи варто зламувати дані того чи іншого підприємства, адже вартість отриманої інформації може не перекрити їхні витрати на підготовку вторгнення.

Інформація — це абстрактне судження, яке поєднує у собі велику кількість значень в залежності від контексту. Простіше кажучи, інформація є змістом даних, які отримав той, хто шукав відповіді на свої запитання.

Інформація буває різноманітною: хибною, правдивою та повною нісенітницею. В залежності від отриманих даних інформація виділяється доступністю для отримувача. Прикладом обмеження є шифр, код — те, що обмежує коло осіб, які зможуть отримати певну інформацію. Інформація може виступати в ролі товару, вона також легко купується і продається (в залежності від попиту на ту чи іншу інформацію).

Варто зазначити, що основними властивостями інформації є цінність, достовірність та актуальність. У свою чергу часовими властивостями інформації постають актуальність, оперативність й ідентичність.

Безпека — це умови, в яких знаходиться складна система, в цих умовах зовнішні та внутрішні чинники, не призводять до негативних процесів, які є згубними для складної системи відповідних потреб, знань і уявлень.

Відповідно, захист інформації — це процес, який спрямований на забезпечення інформаційної безпеки, визначальними факторами якої є загроза (потенційна причина, що знижує рівень інформаційної безпеки системи, тобто потенційно здатну привести до негативних наслідків) і ризик (збиток системи або організації) [11].

Об'єднавши дані визначення, можна сформувати поняття інформаційної безпеки, під яким маємо на увазі рівень захищеності інформаційних джерел, що забезпечують формування суспільства і розвиток в інтересах держави, громадян, організації.

Більш ширшим є визначення автора, який стверджує, що інформаційна безпека — це захищеність особистості при розподілі інформації, держави чи суспільства, внаслідок якої здійснюється їх існування та прогресивний розвиток, незалежно від зовнішніх та внутрішніх загроз [2].

Варто зазначити, що основними цілями інформаційної безпеки є:

конфіденційність, тобто інформація обмежена у доступі і доступна лише обмеженому колу осіб;

виключення несанкціонованого доступу до інформації, коли сторонні особи не можуть ознайомитися або отримати доступ до конфіденційної інформації;

цілісність інформації і належних до неї процесів означає, що інформація повинна бути перевіреною, нерозірваною на "шматки", піддаватися обробці, введенню чи виведенню та не повинна піддаватися ніяким змінам під час даних процесів;

доступність інформації, тобто інформація має бути своєчасною, надійною і, у разі необхідності, бути доступною для уповноважених чи довірених осіб;

встановлення на облік усіх процесів, які пов'язані з ризиком.

У подальшому цілі реалізуються під час вирішення наступних задач:

Передплатний індекс 21847

додавання до системи терміну інформаційної безпеки;

облік та класифікація інформаційних ресурсів організації;

вибір осіб які відповідають за інформаційну безпеку;

визначення ризиків інформаційної безпеки та способів їх мінімізації;

формування групи яка матиме доступ до інформаційних ресурсів;

розробка методів та способів оцінки ризиків, для управління ними;

обирання технічних та адміністративних заходів, які спрямовані на зниження та протидію ризикам;

впровадження заходів, спрямованих на інформаційну безпеку, періодичний контроль за можливими ризиками;

гарантування безпеки працівників та фізичної безпеки;

впровадження нових вимог до інформаційної системи, спираючись на інформаційну безпеку;

контролінг за інформаційною безпекою на підприємстві;

Варто зазначити, що виокремлюють чотири рівні впровадження системи керування інформаційною безпекою:

формування політики галузевих ризиків;

аналіз ризиків для підприємства;

формування кінцевої мети;

розробка політики ризиків включає формування основ керування ними для всієї організації загалом. Дані принципи спираються на цілі підприємства, його стратегію, вимоги, запропоновані законодавством і певними стандартами, спрямованими на інформаційну безпеку [3, с. 120].

Формування системи управління інформаційної безпеки гарантує ефективність, якщо буде сформована на основі міжнародних стандартів ISO/IEC 27001:2005 та ISO/IEC 17799:2005.

Стандарт ISO/IEC 27001:2005 визначає вимоги, яких має дотримуватися підприємство при формуванні інформаційної безпеки підприємства. Вона слідкує за визначення, мінімізацію, керування небезпекою та загрозами, якими може пошкоджуватися інформація, сприяє вибору ефективної та адекватної системи захисту інформації на підприємстві.

Завдяки стандарту ISO/IEC 27001:2005 на підприємстві можливо:

сформувати вимоги та цілі, направлені на інформаційну безпеку;

гарантування впевненості в тому, що керування ризиками в сфері інформаційної безпеки є ефективним та доцільним. Запевнитися в тому, що підприємство діє згідно чинного законодавства і решті нормативних документів;

втілити в життя контроль за функціонуванням системи управління інформаційної безпеки;

виявляти та відстежувати всі існуючі способи управління інформаційною безпекою;

отримання інформації керівництвом щодо стану процесу управління захистом інформації;

регламентацію політики безпеки для внутрішньої та зовнішньої аудиторії шляхом поділу їх на рівні;

забезпечення партнерів та постачальників усією необхідною інформацією про стандарти, процедури та політику підприємства.

Стандарт ISO/IEC 17799:2005 формує принципи та є головним при розробці, впровадженні, супроводі та покращенні системи керування інформаційною безпекою, описує механізм визначення цілей контролінгу і його вартості у таких сферах [4, с. 85]:

політика безпеки (визначення принципів керування і способів, які забезпечують захист інформації);

управління безперервністю бізнес-процесів (виключення сторонніх втручань в ділові операції, захист процесів під час обробки інформації, від втручання серйозних неполадок чи форс-мажорів);

дотримання правових норм (винятки в порушеннях цивільного та кримінального права, встановлених законом зобов'язань, регуляторних чи контрактних зобов'язань, дотримання вимог безпеки);

організація активів та ресурсів (керування захистом інформації всередині підприємства) [5, с. 3];

фізична безпека і безпека навколишнього середовища (виключення несанкціонованого втручання в конфіденційну інформацію);

класифікація і управління активами (знаходження та захист інформаційних ресурсів);

захист персоналу (зменшення ризиків, спричинених помилками оператора, крадіжками, шахрайством чи несанкціоновано використаним обладнанням);

керування доступом (контроль за доступом до інформації);

керування засобами зв'язку та важливим обладнанням;

розробка та обслуговування систем (долучення додаткових засобів до захисту інформаційної системи) [6, с. 18];

Передплатний індекс 21847

Модель системи інформаційної безпеки підприємства — це поєднання внутрішніх та зовнішніх факторів, те як вони впливають на загальний стан інформаційної безпеки на підприємстві та забезпечення безпеки ресурсів.

Фактори, які впливають на систему інформаційної безпеки [7, с. 210]:

— загрози, які мають можливість виникнення та виникають під час формування інформаційної безпеки;

— вразливість інформаційної безпеки, яка прямим чином може призвести до прямих загроз;

— ризики, які є відображенням можливих втрат у разі, якщо загроза стане дійсністю;

Об'єктами захисту є інформаційні та матеріальні ресурси:

— документація, яка збережена на паперових носіях;

— технічні засоби зв'язку та комунікації;

— усна інформація;

— відцифрована інформація, яка може зберігатися та передаватися на різні носії;

— приміщення, в яких проводяться наради та обговорення, зберігання і обробка інформації;

— інформаційні системи загалом, сюди відносяться і системи зв'язку;

— документи, які зберігаються на технічних та програмних засобах;

— програмні засоби;

Усі загрози, з якими зіштовхується підприємство, можна класифікувати за природою їх виникнення, тобто вони можуть бути випадковими або ж навмисними. В залежності від методу боротьби з ними виділяють внутрішні та зовнішні загрози [8, с. 305].

Зовнішніми загрозами є:

— діяльність конкурентів, яка спрямована на перехоплення та обробку важливої інформації;

— випадкові дії працівників сторонніх організацій, які потягли за собою збої у системі інформаційної безпеки;

— умисне знищення, руйнація або ж навмисна модифікація інформації;

— катастрофи і стихійні лиха, непередбачувані ситуації, збої, аварії;

Внутрішніми загрозами є:

— некоординована діяльність структур підприємства, яка спрямована на захист інформації;

— персонал підприємства навмисно знищує інформацію;

— випадкові помилки працівників, застарілість техніки, збої в роботі інформаційної системи;

— грубі порушення правил збору, накопичення, обробки, перетворення, зберігання, відтворення і передавання інформації.

Існує декілька видів порушень [9, с. 11]:

— організаційні види порушень (об'єднують в собі несанкціонований доступ до бази і масових даних, доступ зловмисників до активного мережевого обладнання чи серверів, неправильне розміщення засобів захисту та запобіжників при несанкціонованому доступі або ж помилки при керуванні ними, крадіжка чи небажане ознайомлення із конфіденційною інформацією в паперових чи електронних носіях, розкрадання конфіденційних даних;

— організаційно-правові порушення (спричинені відсутністю об'єднаної політики підприємства, яка була б спрямована на сферу захисту інформації, недотримання вимог нормативних документів, режимів доступу, зберігання і знищення даних);

— фізичні види порушень (нанесення шкоди апаратним засобам, автоматизованим системам, лініям зв'язку, комунікаційному обладнанню, незаконне привласнення або неправомірне ознайомлення із конфіденційною інформацією на носіях або їх викрадення [10, с. 19].

— радіоелектронні види порушень (застосування електронних засобів, які спрямовані на перехоплення та дешифрування потоків інформації, фото чи відео фіксація моніторів та обладнання, поширення дезінформації у локальних мережах, передача даних чужими лініями зв'язку.

Щоб протистояти загрозам та припинити порушення на підприємстві, необхідно організувати процес управління ризиками, який є основою під час побудови системи інформаційної безпеки на підприємстві.

Формування надійної системи інформаційної безпеки — це широкий спектр процедур, спрямованих на мінімізацію внутрішніх та зовнішніх загроз, які обмежені у часі та ресурсах [12, с. 3].

У свою чергу процес керування ризиками включає в себе наступні елементи: опис бізнес-процесів, виявлення ризиків, оцінку ризиків, планування заходів, реалізацію заходів, оцінку ефективності.

Опис бізнес-процесів (аналіз та спостереження за бізнес процесами, визначення критеріїв за якими формуватиметься політика мінімізації ризиків, постійна ідентифікація бізнес процесів) [13, с. 71].

Передплатний індекс 21847

Виявлення ризиків (виявлення ступеня схильності підприємства до загроз, які можуть призвести до вагомої шкоди. Саме для цього і необхідний аналіз бізнес процесів та обговорення з експертами у галузі безпеки. Результатом даного аналізу є класифікація потенційних ризиків).

Стандартними інформаційними ризиками є: копіювання конфіденційної інформації із локальних місць, умисне пошкодження інформації з метою її знищення, копіювання секретних документів для передачі їх конкурентам, незаконний вхід у корпоративну мережу, умисне знищення техніки та обладнання [14, с. 3].

Оцінка ризиків (виокремлення усіх потенційних ризиків із їхніми якісними та кількісними оцінками, які можуть призвести до збитків, виділення ризиків, які не прослідковуються на підприємстві).

Відповідно оцінка ризиків відбувається за наступними етапами:

— опис об'єктів та способів захисту;

— пошук ресурсу і обчислення його кількісних показників;

— аналіз загроз, які можуть зашкодити інформаційній безпеці;

— визначення ступеня вразливості;

— пошук та оцінка засобів забезпечення інформаційної безпеки, які підприємство може використати.

Планування заходів, основною метою яких є встановлення термінів та перелік робіт, які спрямовані на мінімізацію збитків у разі настання критичних моментів [15, с. 48].

Реалізація заходів, тобто виконання всіх запланованих робіт, які пов'язані із мінімізацією ризиків, контроль за якістю отриманих результатів та термінів їх виконання.

Оцінка ефективності — це системний процес, який спрямований на отримання оцінки та об'єктивних матеріалів про поточний стан системи, після проведення всіх запланованих операцій, співвідношення досягнутих результатів із запланованими [16, с. 89].

Отже, управління інформаційною безпекою є досить важкою, відповідальною та клопіткою роботою. Для безпечної діяльності підприємства необхідно ідентифікувати та управляти величезною кількістю інформації. Діяльність, яка спрямована на безпеку, тісно пов'язана із процесом управління ризиками. Необхідно слідкувати за власними інформаційними ресурсами та уважно аналізувати зовнішню інформацію.

ВИСНОВКИ

Для безпечної діяльності підприємства необхідно ідентифікувати та управляти величезною кількістю інформації. Діяльність, яка спрямована на безпеку, тісно пов'язана із процесом управління ризиками. Варто слідкувати за власними інформаційними ресурсами та уважно аналізувати зовнішню інформацію. Таким чином, організаційна модель системи управління інформаційною безпекою підприємства передбачає наявність класичних складових для забезпечення захисту інформаційної інфраструктури товариства: суб'єктів управління інформаційною інфраструктурою та суб'єктів управління інформаційною безпекою, об'єктів, що підлягають цифровому та інформаційному захисту, а також власне процесу управління, який передбачає включення стратегії, політики інформаційної безпеки (неформалізованих), цілей, методів, функцій, заходів та інструментів.

Література:

1. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: монографія. Запоріжжя: ЗІДМУ, 2003. 250 с.

2. Дячков Д.В. Методичні підходи до оцінки інформаційної безпеки підприємства. Вісник Сумського національного аграрного університету: Серія "Економіка і менеджмент". 2017. № 12 (74). С. 87—92.

3. Залевська І. Інформаційна безпека: нові підходи до визначення поняття. Освіта регіону. 2010. № 4. С. 216—219.

4. Захаров Є. Інформаційна безпека: що захищаємо? Свобода висловлювань і приватність. 2013. № 4. С. 3—6.

5. Збожинський С. Інформаційна безпека під час застосування цифрових технологій. Юридична газета. 2017. С. 18—19.

6. Кавун С.В. Інформаційна безпека: підручник. Харків: ХНЕУ, 2009. 368 с.

7. Калетнік В., Калетнік Н. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. Молодий вчений. 2021. С. 305—311.

8. Кісілевич-Чорнойван О.М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. Юриспруденція: теорія і практика. 2009. С. 11—18.

9. Лосєв І. Інформаційна безпека: як укріпити. День. 2014. С. 19.

10. Маракова І.І., Сиропятов О.А. Інформаційна безпека комплексних систем зв'язку.- Ukrainian Information Security Research Journal. 2006. Т.8, № 4.

11. Маркіна І.А., Дячков Д.В. Основи формування системи менеджменту інформаційної

Передплатний індекс 21847

безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. № 3 (1). С. 80—88.

12. Нестеренко О. Свобода інформації чи інформаційна безпека? Свобода висловлювань і приватність. 2011. № 1. С. 3—9.

13. Степанов В. Інформаційна безпека в умовах реалізації інформаційної політики. Вісник Національної академії державного управління при Президентові України. 2019. № 4. С. 71—76.

14. Потапенко О.К. Державна інформаційна політика та безпека. Вісник Київського національного університету імені Тараса Шевченка. Філософія. Політологія. 2011. Вип. 102. С. 48—51.

15. Солодка О. Окремі аспекти правового змісту поняття "інформаційна безпека". Часопис Київського університету права. 2008. № 1. С. 89—93.

16. Федулова С.О. Інформаційна безпека та захист інтелектуальної власності на бази даних. Економічний вісник ДВНЗ "Український державний хіміко-технологічний університет". 2016. С. 189—193.

References:

1. Holubiev, V.O. (2003), Informatsiina bezpeka: problemy borotby z kiberzlochynamy [Information security: problems of combating cybercrimes], ZIDMU, Zaporizhzhia, Ukraine.

2. Diachkov, D.V. (2017), "Methodical approaches to the assessment of information security of the enterprise", Visnyk Sumskoho natsionalnoho ahrarnoho universytetu: Seriia "Ekonomika i menedzhment", vol. 12 (74), pp. 87—92.

3. Zalevska, I. (2010), "Information security: new approaches to the definition of the concept", Osvita rehionu, vol. 4, pp. 216—219.

4. Zakharov, Ye. (2013), "Information security: what are we protecting?", Svoboda vyslovliuvan i pryvatnist, vol. 4, pp. 3—6.

5. Zbozhynskyi, S. (2017), "Information security during the application of digital technologies", Yurydychna hazeta, pp. 18—19.

6. Kavun, S.V. (2009), Informatsiina bezpeka [Information security: a textbook], KhNEU, Kharkiv, Ukraine.

7. Kaletnik, V., and Kaletnik, N. (2021), "Information security and cyber protection as a modern intellectual weapon", Molodyi vchenyi, pp. 305—311.

8. Kisilevych-Chornoivan, O.M. (2009), "Information security and international information security: the problem of defining concepts", Yurysprudentsiia: teoriia i praktyka, pp. 11—18.

9. Losiev, I. (2014), "Information security: how to strengthen it", Den, p. 19.

10. Marakova, I.I. and Syropiatov, O.A. (2006), "Information security of complex communication systems", Ukrainian Information Security Research Journal, vol. 8, no. 4.

11. Markina, I.A. and Diachkov, D.V. (2016), "The basics of the formation of the information security management system of the enterprise", Problemy i perspektyvy rozvytku pidpryiemnytstva, vol. 3 (1), pp. 80—88.

12. Nesterenko, O. (2011), "Freedom of information or information security?" Svoboda vyslovliuvan i pryvatnist, vol. 1, pp. 3—9.

13. Stepanov, V. (2019), "Information security in the conditions of implementation of information policy", Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy, vol. 4, pp. 71—76.

14. Potapenko, O.K., (2011), "State information policy and security", Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Filosofiia. Politolohiia, vol. 102, pp. 48—51.

15. Solodka, O., (2008), "Separate aspects of the legal content of the concept of "information security"". Chasopys Kyivskoho universytetu prava, vol. 1, pp. 89—93.

16. Fedulova, S.O. (2016), "Information security and protection of intellectual property on databases", Ekonomichnyi visnyk DVNZ "Ukrainskyi derzhavnyi khimiko-tekhnolohichnyi universytet", pp. 189—193.

Стаття надійшла до редакції 20.12.2022 р.