УДК 330.341
DOI: 10.31891/2307-5740-2020-284-4-24

МЕЙШ А. В., МАТВІЙЧУК О. В.
Хмельницький національний університет

МЕТОДОЛОГІЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ

У статті проаналізовано та визначено основні загрози інформаційно-комунікативній системі підприємства та їх вплив на діяльність підприємства. Наведено чіткі заходи задля уникнення рейдерства та витоку інформації. Проаналізовані терміни: рейдерство, шахрайство, надана їх характеристика та варіанти зменшення їх на підприємстві.

Ключові слова: інформаційна безпека, рейдерство, інформаційні системи, шахрайство, захист інформації.

MEISH A., MATVIYCHUK O.
Khmelnytskyi National University

METHODOLOGY OF INFORMATION PROTECTION

As you know, the larger the business, the more difficult it becomes to control. In the beginning, its owner or director can keep everything under control, and with its development it becomes difficult for one person to organize all the processes. What aspects should be paid attention to, what past should be excluded, and what is new should be added to the enterprise, what accents should be placed in the control processes - we will reveal in this article.

Any business is a set of certain resources. These include those that have a material expression (real estate, equipment, corporate rights) and those that are expressed in intangible form (information about the activities of the enterprise, its trade secrets).

Qualitatively formed processes are the key to the success of any company.

The development of a modern economy based on the use of new technologies, the creation of new materials, the analysis of large data sets, the development of new management systems leads to a change the principles of competition. Competition has gone beyond traditional notions of competition in existing markets. That's why the purpose of this article is to convey to the head that if his company is promising, it has income, it is already at risk. Raiders have a number of policies, moves that will illegally or even legally leave the company without income. In this article, we have presented recommendations, a number of actions to modernize and move away from the established past, complexes and structures that the company should contain. In the article the problems concerning the directions of the state policy in the field of development of information security are investigated. Based on the analysis of scientific literature in the work it is noted that information security is a state of protection of the individual, society, state from information that is harmful or illegal, from information that has a negative impact on the consciousness of the individual, hinders the sustainable development of the individual, society and state. Thus, before the owner of the enterprise before its immediate opening (the best option) or during the operation of the enterprise there are a number of tasks to which he cannot be irresponsible.

Keywords: information security, raiding, information systems, fraud, information protection.

Постановка проблеми. Як відомо, чим масштабнішим стає бізнес, тим складніше стає його контролювати. На початку тримати все під контролем може його власник чи директор, а вже з його розвитком одній особі стає складно якісно організовувати всі процеси. На які аспекти потрібно звернути увагу, яку минувшину потрібно виключити, а що новітнє потрібно додати на підприємстві, які акценти варто розставляти в процесах контролю – розкриємо у цій статті.

Будь-який бізнес являє собою сукупність певних ресурсів [17]. До них відносяться ті, що мають матеріальне вираження (нерухоме майно, обладнання, корпоративні права), так і ті, що виражені у нематеріальній формі (інформація щодо діяльності підприємства, її комерційні таємниці).

За якісно сформованими процесами лежить ключ до успіху будь-якої компанії.

Аналіз останніх досліджень та публікацій. Актуалізація питань забезпечення інформаційної безпеки різних економічних суб'єктів, включаючи підприємства реального сектору національного господарства, здійснюється в наукових працях І. Арістової, Т. Альшанської, Г. Атаманова, І. Березовської, В. Василюк, О. Дзьобань, О. Додонова, О. Литвиненко, І. Новикової, Л. Фролової, Н. Ястремської та ін. Питанням розроблення і функціонування систем захисту інформації присвячено праці В.Л. Бурячка, В.Б. Дудикевича, М.П. Карпінського, О.С. Петрова, В.О. Хорошка.

Формулювання цілей статті (постановка завдання). Метою роботи є показ нагальності захисту інформації, а також зафіксовані чіткі дії та рекомендації, щоб кожне підприємство, яке розвивається, мало дохід, було в захисті, але для цього, безперечно, потрібно багато роботи.

Викладення основного матеріалу дослідження. XXI століття – це вже не про вартість нерухомого майна, яке належить підприємству, а про захист інформації, яка обробляться ним. Втрата певних відомостей може призвести до різних негативних наслідків. Від витоку клієнтської бази, яку недобросовісні конкуренти можуть використати на власний розсуд, до протиправного заволодіння майном підприємства (так званого, рейдерського захоплення).

Почнемо з того, що юридичного визначення термінів «рейдер» і «рейдерство» в Україні немає. Цікаво виходить: щодня в Україні відбувається захоплення бізнесу, а як його назвати в нас поки не «придумали». Тому, визначити, що таке «рейдерство», ми зможемо за аналогією з тим, що називають «рейдерством» за кордоном, а також трохи «занурившись» в історію. Англійське слово «raid» означає напад, набіг, наліт. При цьому на Заході цим словом називають як законне придбання компанії без згоди власника,

так і силове захоплення з метою зміни власника. У Європі та США поширений тільки перший тип рейдерства, дозволений, контрольований і регульований законом. Однак, якщо взяти Україну, то не завжди рейдери обирають перший спосіб захоплення, оскільки лихі 90-і вклали в підсвідомість зовсім інші правила.

Рейдерство у широкому сенсі – поглинання компанії проти волі її власників (які мають переважне положення на цьому підприємстві) та/або керівника [14, ст. 432]. На практиці (знову ж таки) США, рейдер – це сторона, що «атакує» під час злиття та/або поглинання.

На практиці це поглинання має досить жорсткий вигляд: з підробляннням документів, судових рішень, втручанням у роботу електронних реєстрів і цілою купою інших кримінально караних діянь. Тому компаніям доводиться захищатися, використовуючи для цього комплекс заходів. Можемо почати з того, що цей комплекс заходів – способи всім відомі, не мають нічого незвичного, проте мало хто їх використовує. Більшість думає, що їх компанія ніколи не потрапить до кола потенційних жертв. Якщо це питання торкнулось вас, або ще не торкнулось ці рекомендації в будь-якому випадку будуть корисними [10].

1. Структурування. Воно являється базовим принципом. Структурування – це процес юридичної та податкової оптимізації бізнесу шляхом ефективного поєднання переваг різних юрисдикцій в рамках однієї корпоративної структури, з метою підвищення рентабельності бізнесу та досягнення суміжних завдань. Потрібно розділяти, наприклад, активи в одному місці, господарську діяльність – в іншому. Причому потрібно, щоб компанії-власники не працювали прямо з контрагентами.

2. Корпоративна безпека. Жодна компанія не має нехтувати цим, адже рейдери шукають колишніх співробітників компаній, які можуть бути зацікавлені у співпраці. У компанії має бути набір посадових інструкцій, правил і наказів, при цьому їх треба виконувати.

3. Фізична охорона підприємства. Будь-який бізнес має бути захищений охоронною структурою (яка має відповідні дозволи), готовою зреагувати на інструкції менеджменту й надати фізичний захист активів.

4. Інформаційна безпека й сучасні IT-технології.

Даний перелік – мінімум, який має бути впроваджено в будь-якій компанії, що веде бізнес. Але не варто забувати, що ці заходи відомі й рейдерам, тому на кожний із пунктів є свої (законні/квазізаконні) контрзаходи. Також можна виділити ряд дій, які на перший погляд не є першочерговими, дієвими, але як свідчать джерела будуть ефективними [19, с. 30]:

1. Необхідно скасувати чи для початку обмежити використання печаток. Печатка – рудимент минулого. За ним полювали і полюють всі рейдери. Потрібно відмовлятися від застарілої звички, адже набагато зручніше, а головне безпечніше використовувати електронний підпис [1, с. 43].

2. Електронний підпис. Багато хто скаже, що це не утопія. Безумовно, є операції, які можна підтвердити лише паперовими документами встановленої форми. Але будь-яка фірма може мінімізувати їх рух і обмежити. Найнадійнішим буде апаратний ключ із підписом (тобто на флеш-носії). Лише особисто власник ключа або його довірена особа зможуть підписувати документи таким підписом, таким чином зловмисні дії будуть нівельовані. Також класифікація загроз інформаційній безпеці може бути здійснена поділом загроз на пов'язані із внутрішніми і зовнішніми факторами.

Окремо варто виділити загрози, пов'язані з навмисними помилками, що виникають за межами бізнесу.

До таких загроз відносять:

– несанкціонований доступ до інформації, що зберігається в системі;

– заперечення дій, пов'язаних із маніпулюванням інформацією (наприклад, несанкціонована модифікація, яка веде до порушення цілісності даних);

– введення в програмні продукти і проекти «логічних бомб», які спрацьовують за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп'ютерну систему;

– розроблення і поширення комп'ютерних вірусів;

– недбалість у розробленні, підтримці та експлуатації програмного забезпечення, що призводить до краху комп'ютерної системи;

– зміна комп'ютерної інформації і підробка електронних підписів;

– розкрадання інформації з подальшим маскуванням;

– перехоплення інформаційних потоків;

– заперечення дій або послуги;

– відмова в наданні послуги [6, с. 12].

Як відомо, структуризація – запорука успіху, тому кожна компанія повинна одразу виділяти ці віхи; і тоді безперервна, комплексна робота дасть результати.

Виділимо ці комплекси [5, с. 56].

1. «Попереджений, отже озброєний». Превентивні заходи відіграють істотну роль у системі контролю за обігом інформації на підприємстві. До таких заходів може бути віднесено:

– розробка політики конфіденційності, що повинна бути доведена до відома всіх працівників.

– підписання договорів про конфіденційність із чіткими вимогами щодо фіксування наслідків витоку інформації;

– використання ліцензованого програмного забезпечення для роботи із операційними завданнями бізнесу;

– формування практик зберігання операційних документів у «хмарних середовищах»;

– запровадження електронного документообігу.

2. Людські ресурси. Ця віха – одна з найголовніших, не потрібно цим нехтувати або ретельно підбирати лише керівні посади, важливо розуміти, що наслідки можуть бути дуже серйозні або й навіть фатальні. Корпоративне шахрайство, шпигунство за комерційною інформацією, надання допомоги зовнішнім зловмисникам для рейдерського захоплення бізнесу, булінг серед колективу працівників.

В Європі є частою практикою перевірки кандидатів на поліграфі, це вважають найбільш ефективним інструментом. Поліграфологічне дослідження – це спеціально організований і науково обґрунтований комплекс методів і прийомів їх застосування для отримання, порівняння й інтерпретації психофізіологічних реакцій особи у відповідь на стимули (подразники).

Поліграфні дослідження не підлягають ліцензуванню/патентуванню та не відносяться до медичної практики. Дані дослідження не передбачають отримання спеціальних дозволів та можуть проводитись в рамках звичайної підприємницької діяльності.

3. Нерухоме майно та інші активи, що підлягають реєстрації.

Не менш важливими активами компанії є нерухоме майно та корпоративні права [10]. Вони можуть складати основні виробничі потужності підприємства, а тому їх фактична та юридична втрата може призвести до зупинення діяльності бізнесу. Повертаємось до того ж самого рейдерства. Воно може бути як в фізичній формі, так і на юридичному рівні (через суд можна змінити розподіл часток у статутному капіталі та перереєструвати нерухоме майно). До цього може призвести відсутність належного обліку рухомого майна, не введення в експлуатацію нерухомого майна, недосконала система зберігання установчих документів та печаток компанії, існування практики проставляння підпису керівника замість нього іншими особами. Тепер розглянемо більш ширше поняття – шахрайство [4, с. 109]. Шахрайство – заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Шахрайство – кримінально каране діяння, відповідальність за яке в Україні передбачена Кримінальним кодексом України.

На підприємстві це явище досить небезпечне, оскільки спричиняє багато несприятливих наслідків.

До наслідків можемо віднести: шкоду діловій репутації/бренду; втрата прибутку. Крім того, якщо інформація про ненадійність системи безпеки компанії поширеться серед інших, компанії може бути відмовлено в доступі до публічних закупівель; до компанії можуть бути застосовані заходи кримінально-правового характеру. За наявності факту шахрайства компанія, безумовно, зазнає збитків матеріального характеру, які, на жаль, можуть бути фатальними.

Шахрайство можна поділити на кілька видів:

1) розтрата або розкрадання з боку найманого працівника;

2) шахрайство з боку співкерівників або менеджерів;

3) афери з інвестиціями;

4) шахрайство з боку постачальників;

5) шахрайство з боку замовника або клієнта.

Внутрішнє розслідування у цьому випадку сприятиме боротьбі з втратою коштів, забезпечить обізнаність із внутрішніми процесами й недоліками. Також будь-яке шахрайство залишає за собою юридичний слід, а від так, рано чи пізно, буде викрите (на податковій перевірці, в першу чергу). Це, безумовно, може нести за собою кримінальний характер. Розглянувши види шахрайства, повернемось, знову ж таки, до методів, які здатні запобігти цьому [12, ст.95].

Система відповідальності. Обов'язком керівника є запровадження чіткої політики компанії, яка б передбачала інформацію про відповідальність за порушення цієї політики.

Створивши ефективну систему відповідальності за порушення обов'язків щодо нерозголошення конфіденційної інформації, установивши порядок використання такої інформації, знаючи про відповідальність за порушення наведених порядків, співробітник компанії навряд чи захоче за чашкою кави розповідати своєму приятелю з органів правопорядку про таємниці вашої компанії.

Розділяй або як полюбляють казати в Європі «Не тримайте всі яйця в одному кошику». Тут йде мова передусім про правовстановлюючі документи. Їх необхідно мати в кількох примірниках і зберігати в різних місцях в різних джерелах.

Аналогічно з банківськими рахунками й персоналом. Завжди повинен бути альтернативний банк з альтернативним рахунком. Не можна допускати ситуації, у якій з'являється працівник, заміна якого неможлива або руйнівна для компанії. Як казав Сталін «У нас незамінних людей немає» – так має бути у будь-якій компанії, покладатися можна лише на себе, а з працівниками у вас ринкові відносини.

Стежте за усім. На ринку сьогодення чимало інструментів для постійного моніторингу низки реєстрів та інформаційних баз. Тільки встановлення одної програми може вас убезпечити від фатальних втрат.

Є так званий «маячок», який повідомляє про початок реєстраційних дій. Його функціонал доволі простий і ефективний – у разі намагань внести будь-які зміни до реєстру про це автоматично буде надіслано SMS-повідомлення на визначений номер телефону. Також є багато програм і мобільних застосунків для моніторингу різних баз даних, до того ж критерії моніторингу можуть бути різноманітними.

Цифрування якомога більшої кількості інформації. Ви колись бачили інформацію про успішне рейдерство IT-компанії? Спроби, безперечно, були, але завершилися вони невдачами. Справа в тому, що зараз хмарні технології вже не вважають мейнстрімом, їх ефективно застосовують і це допомагає захистити інформацію, в першу чергу, від фізичного рейдерства.

Збереження всіх даних на віддалених серверах і з достатнім рівнем шифрування є справді хорошим захистом вразливих місць компанії.

Висновки. Розвиток сучасної економіки, заснованої на використанні новітніх технологій, створенні нових матеріалів, аналізі великих масивів даних, розробці нових систем управління призводить до зміни принципів конкурентних відносин. Конкурентна боротьба вийшла за межу традиційних уявлень про суперництво на існуючих ринках. Тому перед кожним власником підприємства, перед його безпосереднім відкриттям стоїть ряд задач, до яких він не може невідповідально віднестись. На основних моментах зупинюсь ще раз. В кожній компанії має бути хороша служба безпеки та якісний юридичний супровід. А також кожний керівник ретельно підбирає персонал, особливо на стратегічно важливі посади, такі як бухгалтер, ІТ-директор, керівник служби безпеки (про метод поліграфу ми згадували вище).

Література

1. Хитарова И. Ю. Духовная жизнь общества как объект информационной безопасности / И.Ю. Хитарова // Этносоциум и межнациональная культура. – 2008. – № 6. – С. 37–47.
2. Конституція України : Основний Закон України від 28.06.1996 № 254к/96-ВР. – URL : http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 02.07.2019).
3. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – К., 2004. – С. 30–33.
4. Красноступ М. Д. Інформаційна безпека України: сутність та проблеми / М.Д. Красноступ // Інформаційні технології та захист інформації. – 1999. – № 1. – С. 108–110.
5. Баранов А. А. Концептуальные вопросы информационной безопасности Украины / А.А. Баранов // Нормативно-правовая база защиты информации : сборник материалов. – К., 1997. – С. 53–58.
6. Згуровський М. З. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення / М.З. Згуровський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – К., 2000. – С. 10–14.
7. Вус М. А. Информационное общество. Информационное право. Информационная безопасность / М.А. Вус, Ю.М. Нестеров // Актуальные проблемы безопасности информационного пространства : материалы Всероссийской научно-практической конференции. СПб, 5-8 октября 1999 г. – СПб, 1999. – С. 19-20.
8. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В.А. Ліпкан. – К. : КНТ, 2006. – 280 с.
9. Данильян О. Г. Національна безпека України: структура та напрямки реалізації : [навчальний посібник] / Данильян О.Г., Дзьобань О.П., Панов М.І. – Х. : Фоліо, 2002. – 285 с.
10. Петраков М. В. Об основных направлениях обеспечения информационной составляющей в системе национальной безопасности / М.В. Петраков // Материалы научной конференции «Концептуальные проблемы информационной безопасности в союзе России и Беларуси». – СПб, 2000. – URL : http://jurfak.spb.ru/ conference/2001.htm (дата звернення: 02.07.2019
11. Основные понятия защиты информации и информационной безопасности. – URL : http://ypn.ru/102/introduction-to-information-protection-and-information-security/ (дата звернення: 02.07.2019).
12. Астахова Л. В. Сущность понятия «Культура информационной безопасности» и ее формирование у студентов вуза / Л. В. Астахова // Экономика. Информатика. Безопасность : сб. науч. тр. Междунар. науч.-практ. конф., 2007 / науч. ред. В. А. Киселева, Л. В. Астахова. – Челябинск : Изд-во ЮУрГУ, 2007. – С. 93–99.
13. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46–48.
14. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін ; [гол. ред. Ю.О. Шпак]. – К. : «МК-Прес», 2005. – 432 с.
15. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2. – Т. 2. – С. 32–35.
16. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем : навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів : Чернігів. нац. технол. ун-т, 2016. – 254 с.
17. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : закон України від 09.01.2007. – URL : http://zakon3.rada.gov.ua/ laws/show/537-16
18. Про службу безпеки України : закон України від 25.03.1992. – URL : http://zakon4.rada.gov.ua/laws/show/2229-12
19. Суббот А. Інформаційна безпека суспільства / А. Суббот // Віче. – 2015. – № 8. – С. 29–31.
20. Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону / К. І. Долженко // Право і Безпека. – 2014. – № 3. – С. 43–48.

References

1. Hitarova I. Yu. Duhovnaya zhizn obshestva kak obekt informacionnoj bezopasnosti / I.Yu. Hitarova // Etnosocium i mezhnacionalnaya kultura. – 2008. – № 6. – S. 37–47.
2. Konstytutsiia Ukrainy : Osnovnyi Zakon Ukrainy vid 28.06.1996 № 254k/96-VR. – URL : http://zakon3.rada.gov.ua/ laws/show/254%D0%BA/96-%D0%B2%D1%80 (data zvernennia: 02.07.2019).
3. Tsymbaliuk V. Okremi pytannia shchodo vyznachennia katehorii «informatsiina bezpeka» u normatyvno-pravovomu aspekti / V. Tsymbaliuk // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini : naukovo-tekhnichnyi zbirnyk. – K., 2004. – S. 30–33.
4. Krasnostup M. D. Informatsiina bezpeka Ukrainy: sutnist ta problemy / M.D. Krasnostup // Informatsiini tekhnolohii ta zakhyst informatsii. – 1999. – № 1. – S. 108–110.
5. Baranov A. A. Konceptualnye voprosy informacionnoj bezopasnosti Ukrainy / A.A. Baranov // Normativno-pravovaya baza zashity informacii : sbornik materialov. – K., 1997. – S. 53–58.
6. Zghurovskyi M. Z. Problemy informatsiinoi bezpeky v Ukraini, shliakhy yikh vyrishennia / M.Z. Zghurovskyi // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini : naukovo-tekhnichnyi zbirnyk. – K., 2000. – S. 10–14.
7. Vus M. A. Informacionnoe obshestvo. Informacionnoe pravo. Informacionnaya bezopasnost / M.A. Vus, Yu.M. Nesterov // Aktualnye problemy bezopasnosti informacionnogo prostranstva : materialy Vserossijskoj nauchno-prakticheskoj konferencii. SPb, 5-8 oktyabrya 1999 g. – SPb, 1999. – S. 19-20.
8. Lipkan V. A. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii : [navchalnyi posibnyk] / V.A. Lipkan. – K. : KNT, 2006. – 280 s.
9. Danylian O. H. Natsionalna bezpeka Ukrainy: struktura ta napriamky realizatsii : [navchalnyi posibnyk] / Danylian O.H., Dzoban O.P., Panov M.I. – Kh. : Folio, 2002. – 285 s.

10 Petrakov M. V. Ob osnovnyh napravleniyah obespecheniya informacionnoj sostavlyayushej v sisteme nacionalnoj bezopasnosti / M.V. Petrakov // Materialy nauchnoj konferencii «Konceptualnye problemy informacionnoj bezopasnosti v soyuze Rossii i Belarusi». – SPb, 2000. – URL : http://jurfak.spb.ru/ conference/2001.htm (data zvernennya: 02.07.2019

11. Osnovnye ponyatiya zashity informacii i informacionnoj bezopasnosti. – URL : http://ypn.ru/102/introduction-to-information-protection-and-information-security/ (data zvernennya: 02.07.2019).

12. Astahova L. V. Sushnost ponyatiya «Kultura informacionnoj bezopasnosti» i ee formirovanie u studentov vuza / L.V. Astahova // Ekonomika. Informatika. Bezopasnost : sb. nauch. tr. Mezhdunar. nauch.-prakt. konf., 2007 / nauch. red. V. A. Kiseleva, L. V. Astahova. – Chelyabinsk : Izd-vo YuUrGU, 2007. – S. 93–99.

13. Horbatiuk O.M. Suchasnyi stan ta problemy informatsiinoi bezpeky Ukrainy na rubezhi stolit / O.M. Horbatiuk // Visnyk Kyivskoho universytetu imeni T. Shevchenka. – 1999. – Vyp. 14: Mizhnarodni vidnosyny. – S. 46–48.

14. Bohush V. Informatsiina bezpeka derzhavy / V. Bohush, O. Yudin ; [hol. red. Yu.O. Shpak]. – K. : «MK-Pres», 2005. – 432 s.

15. Sorokivska O.A. Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy / O.A. Sorokivska, V.L. Hevko // Visnyk Khmelnytskoho natsionalnoho universytetu. – 2010. – № 2. – T. 2. – S. 32–35.

16. Lytvynov V.V. Modeliuvannia ta analiz bezpeky rozpodilenykh informatsiinykh system : navch. pos. [dlia stud. spets. 121 «Inzheneriia prohramnoho zabezpechennia»] / V.V. Lytvynov, V.V. Kazymyr, I.V. Stetsenko ta in. – Chernihiv : Chernihiv. nats. tekhnol. un-t, 2016. – 254 s.

17. Pro osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 rr. : zakon Ukrainy vid 09.01.2007. – URL : http://zakon3.rada.gov.ua/ laws/show/537-16

18. Pro sluzhbu bezpeky Ukrainy : zakon Ukrainy vid 25.03.1992. – URL : http://zakon4.rada.gov.ua/laws/show/2229-12

19. Subbot A. Informatsiina bezpeka suspilstva / A. Subbot // Viche. – 2015. – № 8. – S. 29–31.

20. Dolzhenko K. I. Normatyvno-pravove rehuliuvannia informatsiinoi bezpeky rehionu / K. I. Dolzhenko // Pravo i Bezpeka. – 2014. – № 3. – S. 43–48.

Надійшла / Paper received: 17.08.2020 Надрукована / Paper Printed : 30.09.2020