Адміністративне право і процес; фінансове право; інформаційне право

УДК 34.096

Шепета Олена Василівна
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України
Шепета Елена Васильевна
кандидат юридических наук, доцент,
доцент кафедры организации защиты информации с ограниченным доступом
Учебно-научный институт информационной безопасности
Национальной академии Службы безопасности Украины
Shepeta Olena
PhD in Law, Associate Professor,
Associate Professor of Defense restricted information Department
Educational and Scientific Institute of Information Security of the
National Academy of Security Service of Ukraine

Тугарова Оксана Кузьмівна
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України
Тугарова Оксана Кузьминична
кандидат юридических наук, доцент,
доцент кафедры организации защиты информации с ограниченным доступом
Учебно-научный институт информационной безопасности
Национальной академии Службы безопасности Украины

Tugharova Oksana

PhD in Law, Associate Professor,

Associate Professor of Defense restricted information Department at

Educational and Scientific Institute of Information Security of the

National Academy of Security Service of Ukraine

ОСНОВНІ ВИМОГИ ДО ПЛАНУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ПІДПРИЄМСТВІ

ОСНОВНЫЕ ТРЕБОВАНИЯ К ПЛАНИРОВАНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУКАЦИОННЫХ СИСТЕМАХ НА ПРЕДПРИЯТИИ

BASIC REQUIREMENTS FOR INFORMATION PROTECTION PLANNING IN INFORMATION AND TELECOMMUNICATION SYSTEMS AT AN ENTERPRISE

Анотація. *Сьогодні, захист інформації на підприємстві, перетворюється на одну з найактуальніших задач у зв'язку із надзвичайно широким використанням різноманітних систем обробки інформації, розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації комерційного характеру, власник якої був би категорично проти ознайомлення з нею сторонніх осіб. Проаналізувавши наукові публікацій можна дійти висновку, що із збільшенням обробки інформації в інформаційно-телекомунікаційних системах на підприємстві обов'язково треба створювати службу захисту інформації. Діяльність служби захисту інформації підприємства повинна плануватись і регулюватись нормативно-правовими актами, які створюються і затверджуються керівництвом підприємства в основі яких доцільно дотримуватись національних правових норм інформаційної*

безпеки та використовувати рекомендації міжнародних стандартів серії ISO 2700.

Створення служби захисту інформації на підприємстві має за мету організаційне забезпечення наступних завдань, таких як: планування, керування комплексною системою захисту інформації в інформаційно-телекомунікаційних системах та здійснення контролю за її функціонуванням.

Служба захисту інформації повинна здійснювати свою діяльність відповідно до «Плану захисту інформації в інформаційно-телекомунікаційних системах», календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) підприємства. План захисту інформації в інформаційно-телекомунікаційних системах є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу інформаційно-телекомунікаційної системи.

На підприємствах, де штатним розкладом не передбачено створення служби захисту інформації, заходи щодо забезпечення захисту інформації в інформаційно-телекомунікаційних системах можуть здійснювати призначені наказом керівника підприємства працівники [4].

Ключові слова: *служба захисту інформації, інформаційно-телекомунікаційна система, підприємство, класифікація інформації, комплексна система захисту інформації в інформаційно-телекомунікаційних системах.*

Аннотация. *Сегодня, защита информации на предприятии, превращается в одну из самых актуальных задач в связи с чрезвычайно широким использованием различных систем обработки информации, расширение локальных и глобальных компьютерных сетей, по которым передаются огромные объемы информации коммерческого характера,*

владелец которой был бы категорически против ознакомления с ним посторонних лиц. Проанализировав научные публикаций можно сделать вывод, что с увеличением обработки информации в информационно-телекоммуникационных системах на предприятии обязательно надо создавать службу защиты информации. Деятельность службы защиты информации предприятия должна планироваться и регулироваться нормативно-правовыми актами, которые создаются и утверждаются руководством предприятия в основе которых целесообразно придерживаться национальных правовых норм информационной безопасности и использовать рекомендации международных стандартов серии ISO 2700.

Создание службы защиты информации на предприятии имеет целью организационное обеспечение следующих задач, таких как: планирование, управление комплексной системой защиты информации в информационно-телекоммуникационных системах и осуществления контроля за его функционированием.

Служба защиты информации должна осуществлять свою деятельность в соответствии с «Планом защиты информации в информационно-телекоммуникационных системах», календарных, перспективных и других планов работ, утвержденных руководителем (заместителем руководителя) предприятия. План защиты информации в информационно-телекоммуникационных системах является совокупностью документов, согласно которым осуществляется организация защиты информации на всех этапах жизненного цикла информационно-телекоммуникационной системы.

На предприятиях, где штатным расписанием не предусмотрено создание службы защиты информации, меры по обеспечению защиты информации в информационно-телекоммуникационных системах могут

осуществлять назначенные приказом руководителя предприятия работники [4].

Ключевые слова: *служба защиты информации, информационно-телекоммуникационная система, предприятие, классификация информации, комплексная система защиты информации в информационно-телекоммуникационных системах.*

Summary. *Today, the information protection at any enterprise is becoming one of the most urgent tasks because of the extremely wide use of various information processing systems, expansion of local and global computer networks, which transmit huge amounts of commercial information, which is owned by one who would not like any stranger to be acquainted with it.*

After analyzing scientific publications, we have come to the conclusion that with the increase of information processing in information and telecommunication systems, there is an urgent need to create an information protection service at an enterprise. The activities of the company's information protection service should be planned and regulated by local norms created and approved by the company's management, based on which it is advisable to comply with national legal norms of information security and use the recommendations of ISO 2700 series' international standards.

The creation of the information protection service at the enterprise aims at organizational support of the following tasks, such as: planning, management of the complex system of information protection in information and telecommunication systems and control over its functioning. The information protection service must carry out its activities in accordance with the "Information Protection Plan in Information and Telecommunication Systems", calendar, long-term and other work plans approved by the head (deputy head) of the enterprise.

The information protection plan in information and telecommunication systems is a set of documents according to which the information protection organization at all stages of the information and telecommunication system life cycle is being carried out.

In enterprises where the staffing schedule does not provide for the establishment of an information security service, measures to ensure the information protection in information and telecommunications systems may be carried out by employees appointed by the head of the enterprise' order [4].

Key words: *information protection service, information and telecommunication system, enterprise, information classification, complex information protection system in information and telecommunication systems.*

Постановка проблеми. У зв'язку із пандемією коронавірусу «COVID-19», більшість українських підприємств запровадили введення онлайн-бізнесу, що свідчить про те що в своїй діяльності вони використовують новітні досягнення Інтернет технологій.

Тому при введенні в дію новітніх технологій на підприємстві інформація стає врази цінною. Відповідно зростає активність різного виду порушників. Створення служби захисту інформації дає гарантію забезпечення комплексного захисту інформації та контролю за її функціонуванням на підприємстві.

Служба захисту інформації здійснює свою роботу з реалізації основних завдань на підставі «Плану захисту інформації в інформаційно-телекомунікаційних системах».

Аналіз останніх досліджень і публікацій. Питаннями організації захисту інформації на підприємствах, установах та організаціях присвячено значну кількість праць Марущака А.І. [7], Дудкевича В.Б. [9], Хорошка В.О. [8].

Аналіз наукових публікацій дає підстави стверджувати, що із запровадженням новітніх інформаційних технологій на підприємстві обов'язково треба створювати «План захисту інформації в інформаційно-телекомунікаційних системах».

Формулювання цілей статті (постановка завдання). Метою цієї статті є перегляд основних вимог до планування захисту інформації в інформаційно-телекомунікаційних системах на підприємстві з урахуванням сучасних загроз.

Виклад основного матеріалу. План захисту інформації в інформаційно-телекомунікаційних системах (далі – План захисту) розробляється на підставі проведеного аналізу технології обробки інформації на підприємстві, аналізу ризиків, сформульованої політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в інформаційно-телекомунікаційних системах, основні завдання захисту, загальні правила обробки інформації в інформаційно-телекомунікаційних системах, мету побудови та функціонування комплексної системи захисту інформації, заходи з захисту інформації. План захисту має фіксувати на певний момент часу склад інформаційно-телекомунікаційної системи, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації та ін. [4].

План захисту повинен складатись з наступних розділів:

- завдання захисту інформації в АС;
- класифікація інформації, що обробляється в АС;
- опис компонентів АС та технології обробки інформації;
- загрози для інформації в АС;
- політика безпеки інформації в АС;
- система документів з забезпечення захисту інформації в АС [4].

Так до завдань із захисту інформації можна віднести: забезпечення визначеної політики безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації інформаційно-телекомунікаційної системи; своєчасне виявлення та знешкодження загроз для ресурсів інформаційно-телекомунікаційної системи, причин та умов, які спричиняють, або можуть привести до порушення її функціонування та розвитку; створення механізму та умов оперативного реагування на загрози для безпеки інформації; ефективне знешкодження, або попередження загроз для ресурсів інформаційно-телекомунікаційної системи шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки; керування засобами захисту інформації, керування доступом користувачів до ресурсів інформаційно-телекомунікаційної системи, контроль за їхньою роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби несанкціонований доступ до ресурсів інформаційно-телекомунікаційної системи; реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації; створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними або несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування інформаційно-телекомунікаційної системи.

Також повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в інформаційно-телекомунікаційних системах. Класифікація є підставою для визначення власником інформації методів і способів захисту кожного окремого виду інформації [4].

За режимом доступу інформація в інформаційно-телекомунікаційної

системи має бути поділена на: відкриту та з обмеженим доступом.

Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави [6], відкриту інформацію, вимога щодо захисту якої встановлена законом важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну, службову, конфіденційну.

До таємної інформації має бути віднесена інформація, що містить відомості, які становлять комерційну таємницю.

Правила доступу до службової інформації та інформації, вимога щодо захисту якої встановлена законом, встановлюється її власником згідно з вимогами нормативно-правових актів.

Правила доступу до конфіденційної інформації встановлюють фізичні та юридичні особи, у володінні яких вона перебуває. Конфіденційна інформація може мати велику цінність, втрата або передача якої іншим особам може завдати організації (розпоряднику) значних збитків. З метою встановлення правил розмежування доступу до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за ступенем цінності.

Необхідно провести інвентаризацію усіх компонентів інформаційно-телекомунікаційних систем і зафіксувати всі об'єкти, які беруть участь у технологічному процесі обробки, які тим чи іншим чином впливають на безпеку інформації.

До об'єктів, що підлягають інвентаризації, можуть бути віднесені: обладнання (процесори, монітори, термінали та ін.), периферійні пристрої; програмне забезпечення, операційні системи та інші системні програми,

діагностичні і тестові програми тощо; дані - тимчасового і постійного зберігання, друковані, архівні і резервні копії, системні журнали, технічна, експлуатаційна і розпорядча документація та ін.; персонал і користувачі інформаційно-телекомунікаційних систем.

Для проведення аналізу ризиків при обробці інформації та формування вимог до комплексної системи захисту інформації на підприємстві є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в інформаційно-телекомунікаційної системи: технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали; каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Загрози для інформації, що обробляється в інформаційно-телекомунікаційній системі, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно інформаційно-телекомунікаційної системи і повинні враховуватись у моделі загроз,

наприклад: зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події); збої і відмови у роботі обладнання та технічних засобів інформаційно-телекомунікаційної системи; наслідки помилок під час проектування та розробки компонентів інформаційно-телекомунікаційної системи (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо); помилки користувачів інформаційно-телекомунікаційної системи під час експлуатації; навмисні дії потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості інформаційно-телекомунікаційної системи [4].

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути: дії, що призводять до відмови інформаційно-телекомунікаційної системи, руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.); ненавмисне пошкодження носіїв інформації; неправомірна зміна режимів роботи інформаційно-телекомунікаційної системи (окремих компонентів, обладнання, програмне забезпечення тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації); неумисне зараження програмного забезпечення комп'ютерними вірусами; невиконання вимог до організаційних заходів захисту чинних в інформаційно-телекомунікаційній системі розпорядчих документів; помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо; будь-які дії, що можуть призвести до

розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо; неправомірне впровадження і використання забороненого політикою безпеки програмного; наслідки некомпетентного застосування засобів захисту; інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи інформаційно-телекомунікаційної системи або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути: порушення фізичної цілісності інформаційно-телекомунікаційної системи; порушення режимів функціонування систем життєзабезпечення інформаційно-телекомунікаційної системи (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.); порушення режимів функціонування інформаційно-телекомунікаційної системи (обладнання і програмного забезпечення); впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки; використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів; використання (шантаж, підкуп тощо) з корисливою метою персоналу інформаційно-телекомунікаційної системи; крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо); несанкціоноване копіювання носіїв інформації; неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо; впровадження і використання забороненого політикою безпеки програмного забезпечення або несанкціоноване використання програмного забезпечення, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж); інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної інформаційно-телекомунікаційної системи. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до інформаційно-телекомунікаційної системи порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати: можливу мету порушника та її градацію за ступенями небезпечності для інформаційно-телекомунікаційної системи; категорії осіб, з числа яких може бути порушник; припущення про кваліфікацію порушника; припущення про характер його дій.

Метою порушника можуть бути: отримання необхідної інформації у потрібному обсязі та асортименті; мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами); нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Під політикою безпеки інформації на підприємстві (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Політика безпеки інформації в інформаційно-телекомунікаційних системах підприємства є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості

обчислювальних систем, фізичного середовища та інші чинники. В інформаційно-телекомунікаційної системи може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в інформаційно-телекомунікаційної системи мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів інформаційно-телекомунікаційної системи), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування [4].

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

Політика безпеки розробляється на підготовчому етапі створення комплексної системи захисту інформації на підприємстві [5].

Регулятивно-правову основу у вирішенні проблем захисту інформації в інформаційно-телекомунікаційних системах підприємств України різної форм власності становлять: Конституція України [1], відповідні закони України, нормативно-правові акти Президента України і Кабінета Міністрів України, інші нормативно-правові акти з питань захисту інформації, державні і галузеві стандарти, розпорядчі та інші документи організації [2; 3]. Також доцільно використовувати наступні рекомендації міжнародних стандартів з організації захисту інформації.

Такими міжнародними стандартами є: ISO/IEC 27002 «Інформаційні технології. методи захисту. Кодекс практики для управління інформаційною безпекою»; ISO/IEC 27003 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту

захисту інформації»; ISO/IEC 27004 «Інформаційні технології. Методи захисту. Вимірювання»; ISO/IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки»; ISO/IEC 27006 «Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систему правління інформаційною безпекою»; ISO/IEC 27011 «Інформаційні технології. Керівництво з управління інформаційною безпекою для телекомунікацій».

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Підсумовуючи все вище наведене, зробимо висновок, що створення Плану захисту інформації в інформаційно-телекомунікаційних системах є дуже складне і кропітке завдання, яке стоїть перед службою захисту інформації підприємства, при вирішенні якого потрібного врахувати багато різних чинників для якісного функціонування інформаційно-телекомунікаційної системи. А також й на далі треба розвивати напрямок захисту інформації для якісної роботи підприємства, тому що інформаційні технологій великими кроками йдуть вперед.

Література

1. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.
2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 № 81/94-ВР . Дата оновлення 04.07.2017. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 19.08.2020).
3. Про інформацію : Закон України від 02.10.1992 року №2657-XII . Дата оновлення 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 19.08.2020).

4. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. (Чинний від 04.12.2000р., зі змінами від 28.12.2012 № 806). (Інформація та документація).
5. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. (Чинний від 28.04.1999 р., зі змінами від 28.12.2012 № 806). (Інформація та документація).
6. Концепція технічного захисту інформації : Постанова Кабінету міністрів України від 08.10.97 № 1126-97п. Дата оновлення 13.10.2011. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text (дата звернення 25.02.2021).
7. Марущак А. Скицько О. Вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання / А. Марущак, О. Скицько // Безпека інформації. 2018. Т.24, № 1. С.69-74. URL: http://nbuv.gov.ua/UJRN/bezin_2018_24_1_12
8. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Киев: Издательство «Юниор», 2003. 504 с.
9. Дудкевич Б. Пасивний захист інформації від лазерного зондування / В. Б. Дудикевич, І. С. Собчук, В. О. Ракобовчук // Вісник Національного університету "Львівська політехніка". Сер.: Автоматика, вимірювання та керування. 2013. № 753. С. 118-123. URL: http://nbuv.gov.ua/UJRN/VNULP_2013_753_20.

References

1. The Constitution of Ukraine: official text. Kyiv: KM, 2013. 96 p.
2. On information protection in information and telecommunication systems: Law of Ukraine of 05.07.94 № 81/94-VR. Date of update 04.07.2017. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (access date: 19.08.2020).

3. On information: Law of Ukraine of October 2, 1992 №2657-XII. Date of update 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (access date: 19.08.2020).
4. ND TZI 1.4-001-2000 Standard regulations on information protection service in the automated system. (Actual from 04.12.2000, with changes from 28.12.2012 № 806). (Information and documentation).
5. ND TZI 3.7-001-99 Methodical instructions on development of the technical task on creation of complex system of protection of the information in the automated system. (Actual from 28.04.1999, with changes from 28.12.2012 № 806). (Information and documentation).
6. The concept of technical protection of information: Resolution of the Cabinet of Ministers of Ukraine from 08.10.97 № 1126-97p. Date of update 13.10.2011. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text (access date 25.02.2021).
7. Marushchak A. Skitsko O. Influence of shadow information technologies on information security of the business entity / A. Marushchak, O. Skitsko // Information security. 2018. Vol.24, № 1. P. 69-74 URL: http://nbuv.gov.ua/UJRN/bezin_2018_24_1_12.
8. Khoroshko V.A., Chekatkov A.A. Methods and means of information protection. Kiev: Publishing House "Junior", 2003. 504 p.
9. Dudkevych B. Passive protection of information from laser sounding / V.B. Dudykevych, I.S. Sobchuk, V.O. Rakobovchuk // Bulletin of the National University "Lviv Polytechnic". Ser. : Automation, measurement and control. 2013. № 753. P. 118-123. URL: http://nbuv.gov.ua/UJRN/VNULP_2013_753_20.