цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі [4].

Висновки. Отже, захист інформації на підприємстві є доцільним здійснювати в наступних напрямах: комплексним застосуванням різних засобів і методів; створенням структури захисту й охорони з кількома рівнями; постійним їх удосконаленням.

Успіх справи залежить від збалансованої й налагодженої взаємодії захисту операційних систем і гарантування безпеки баз даних.

Список використаних інформаційних джерел

1. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / М. І. Зубок. – Київ : КНТЕУ, 2005. – 76 с.
2. Інформаційне законодавство: збірник законодавчих актів / ред. Ю. С. Шемшученко, К. С. Чиж. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – Київ: Юридична думка, 2005. – 328 с.
3. Карпенко О. О. Сучасне діловодство : навч. посіб. / О. О. Карпенко, М. М. Матліна. – Харків : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 75 с.
4. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] / Ю. О. Коваленко. – Режим доступу: http://www.econindustry.org/arhiv/html/2010/st_51_ 18.pdf (дата звернення: 05.10.2019). – Назва з екрана.

УДК 351.746:007

БЕЗПЕКА ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ УСТАНОВИ

І. О. Славко, *магістр спеціальності 029 Інформаційна, бібліотечна та архівна справа освітня програма «Документознавство та інформаційна діяльність»*
М. В. Макарова, *д. е. н., професор – науковий керівник*

Анотація. Розглянуто поняття інформаційної безпеки, її базові рівні. Зазначено відповідність завдань інформаційної безпеки установи Доктрині інформаційної безпеки України. Означено

види інформації, що підлягає захисту. Наведено складові плану захисту інформації відповідно до Правил забезпечення захисту інформації в інформаційних та інших системах. Визначено роль Державної служби спеціального зв'язку та захисту інформації України в організації безпеки документно-інформаційної системи установи, що є однією з ланок інформаційного захисту держави в цілому.

Ключові слова: безпека інформаційної системи, інформаційний захист, Доктрина інформаційної безпеки, план захисту, служба захисту.

Abstract. The concept of information security, its basic levels are considered. The compliance of the institution's information security tasks with the Doctrine of Information Security of Ukraine is indicated. The types of information to be protected are identified. The components of the information security plan according to the Rules for providing information protection in information and other systems are given. The role of the State Service for Special Communication and Information Protection of Ukraine in the organization of the security of the institution's document-information system, which is one of the part of information protection of the state as a whole, is determined.

Key words: information system security, information security, Doctrine of Information Security, security plan, security service.

Постановка проблеми. В умовах сьогодення роль інформаційної безпеки на різних рівнях невпинно зростає. Однією з передумов цього є швидкий темп інформатизації суспільства, оскільки захищеність організації від інформаційних впливів залежить від рівня її інформаційного розвитку. Виникнення нових ризиків спричиняє пошук нових шляхів вдосконалення захисту документно-інформаційних ресурсів.

Аналіз основних досліджень і публікацій. Питанням захисту інформації приділяли увагу українські вчені, зокрема М. В. Гайворонський та О. М. Новіков присвятили свої праці питанню безпеки інформаційно-комунікаційних систем та аналізу загроз, В. С. Галатенко розглянув засади інформаційної безпеки, О. В. Курбан особливу увагу приділяв національній інфор-

маційній безпеці держави, В. М. Петрик присвятив свої роботи інформаційній безпеці не лише особи чи організації, але й у масштабах держави, а А. Ю. Щеглов розглянув питання захисту комп'ютерної інформації від несанкціонованого доступу.

Формулювання мети. Метою статті є визначення основних засад організації безпеки документно-інформаційних систем установ.

Виклад основного матеріалу дослідження. Інформаційна безпека – це комплексне поняття. Відповідно до законодавства України, під інформаційною безпекою розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [4].

Згідно [3] визначаються три базових рівня інформаційної безпеки, а саме: рівень особи, що передбачає формування раціонального, критичного мислення на основі принципів свободи вибору; суспільний рівень, який полягає у формуванні якісного інформаційно-аналітичного простору, багатоканальність отримання інформації, незалежні ЗМІ; державний рівень, що вміщує інформаційно-аналітичну роботу органів, інформаційне забезпечення внутрішньої та зовнішньої політики на міждержавному рівні, систему захисту інформації, протидію правопорушенням в інформаційній сфері. З огляду на це захист інформації усіх державних органів та організацій є важливою складовою загального стану безпеки, а отже, стає ще вагомішим.

Доктриною інформаційної безпеки України задекларовано, що життєво важливими інтересами суспільства і держави серед інших є всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток і захист національної інформаційної інфраструктури та ін. Пріори-

тетами державної політики щодо забезпечення інформаційної безпеки мають бути [1]:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави;

– визначення механізмів регулювання роботи підприємств, установ, організацій та ін.

Отже, організація захисту документно-інформаційної системи установ є дотриманням принципів згаданої вище Доктрини.

У Правилах забезпечення захисту інформації в інформаційних та інших системах [5] окреслено вимоги до забезпечення захисту інформації в системі та організаційні засади забезпечення захисту інформації. Зокрема, захист інформації на всіх етапах створення та експлуатації документно-інформаційної системи здійснюється відповідно до розробленого службою захисту інформації установи плану, складові якого подано на рисунку 1.

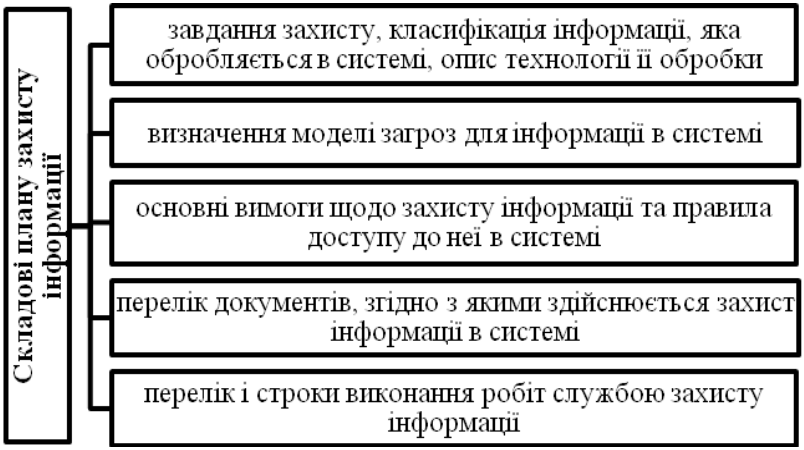

Рисунок 1 – Складові плану захисту інформації установи. Складено автором на основі [5]

Вирішенням проблеми захисту документно-інформаційної системи установи є створення комплексної системи захисту інформації, яка є сукупністю «організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку й несанкціонованого доступу» [2]. Комплексність дозволяє передбачити різні види загроз безпеці, що є передумовою для ефективного захисту документно-інформаційних ресурсів.

Для кожної конкретної документно-інформаційної системи склад, структура та вимоги до системи захисту інформації визначаються властивостями оброблюваної інформації та актуальними загрозами безпеки. Також важливим аспектом є автоматизованість системи документообігу установи.

Розробка системи захисту інформації складається з організаційних та інженерно-технічних заходів. Організаційні заходи полягають у розробці посадових інструкцій для користувачів та обслуговуючого персоналу, створенні правил функціонування інформаційної системи, забезпеченні засобів ідентифікації користувачів, розробці планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи тощо. Сутність інженерно-технічних заходів полягає у технічному забезпеченні процесу, а саме створення служби захисту інформації, фізична оборона об'єктів, визначення порядку дій та поведінки користувачів, технічні заходи, засоби криптографічного характеру тощо [2]. Від досконалості системи залежить рівень захищеності інформації установи, тому її розробці та актуалізації слід приділяти значну увагу.

Висновки. Організація документно-інформаційної безпеки установи є продовженням державної політики в галузі інформаційного захисту та необхідною передумовою розвитку та функціонування будь-якої організації. Принципи та правила захисту інформації задекларовані, але важливу роль має їх реалізація на кожному із суб'єктів у межах створення комплексної системи захисту, тому розробка шляхів для зростання рівня захищеності документно-інформаційних систем установи є предметом подальших досліджень.

Список використаних інформаційних джерел

1. Доктрина інформаційної безпеки України [Електронний ресурс] : Затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. – Режим доступу: https://zakon5.rada.gov.ua/laws/show/47/2017 (дата звернення: 22.09.19). – Назва з екрана.
2. Захист інформаційних систем – важливе завдання сьогодення [Електронний ресурс]. – Режим доступу: http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/ (дата звернення: 20.09.19). – Назва з екрана.
3. Курбан О. В. Основи сучасної національної інформаційної безпеки України // Вісник Харківської державної академії культури. Серія: Соціальні комунікації. – 2017. Випуск 50. – С. 55–66.
4. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик // Юридичний журнал. – 2009. – № 5. – Режим доступу: https://web.archive.org/web/20150710023330/http://www.justinian.com.ua/article.php?id=3222 (дата звернення: 22.09.19). – Назва з екрана.
5. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – Режим доступу: https://www.kmu.gov.ua/ua/npas/32791826 (дата звернення: 19.09.19). – Назва з екрана.