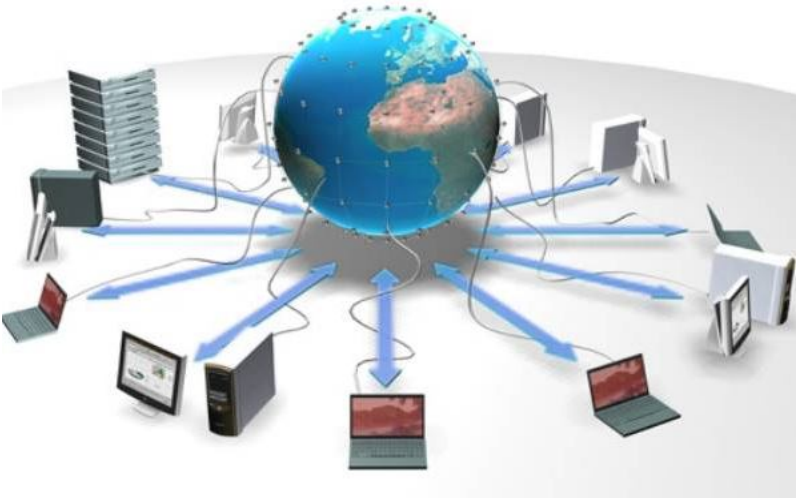
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ І УПРАВЛІННІ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 1



Одеса
2019

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сохадзе Т. Т.[1], **Орлик О. В.**[2]

1 – студентка 3 курсу 33 гр., факультет міжнародної економіки,
2 – канд. екон. наук, доцент, кафедра економічної кібернетики та інформаційних технологій
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Сохадзе Т. Т., Орлик О. В. ***Методи забезпечення безпеки інформації в інформаційних системах.*** *Виділені види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій. Визначено сукупність сучасних методів захисту інформації в інформаційних системах та проведено аналіз особливостей їх застосування.*

Ключові слова: *інформаційна безпека, інформація, інформаційна система, захист інформації, методи захисту.*

Сохадзе Т. Т., Орлик О. В. ***Методы обеспечения безопасности информации в информационных системах.*** *Выделены виды потенциальных угроз безопасности деятельности предприятия в сфере информационных технологий. Определена совокупность современных методов защиты информации в информационных системах и проведен анализ особенностей их применения.*

Ключевые слова: *информационная безопасность, информация, информационная система, защита информации, методы защиты.*

Sokhadze T. T., Orlyk O. V. ***Methods of ensuring the security of information in information systems.*** *There are highlighted some types of potential security threats in the field of information technology. The set of modern methods of information protection in information systems is determined and the analysis of the features of their application is carried out.*

Keywords: *information security, information, information system, information protection, methods of protection.*

ПОСИЛАННЯ НА РЕСУРС

Сохадзе Т. Т., Орлик О. В. *Методи забезпечення безпеки інформації в інформаційних системах* // Інформаційні технології в економіці і управлінні : зб. наук. студ. праць. Одеса : ОНЕУ, 2019. Вип. 1. С. 84–88.

Постановка проблеми у загальному вигляді. За умов нестачі матеріальних ресурсів природи, інформація стає найважливішим ресурсом для розвитку і функціонування суспільства. У сучасному світі інформація є дуже важливим стратегічним ресурсом, який забезпечує майбутній розвиток будь-якого підприємства. Виходячи з цього, як усі інші ресурси, інформація потребує надійного захисту.

У сучасному суспільстві широко використовуються автоматизовані інформаційні системи (АІС). Через зростаючу роль інформаційних ресурсів у житті сучасної людини, а також через актуальність численних загроз, проблема безпеки інформаційних систем (ІС) набула важливого значення і вимагає постійної уваги.

Аналіз досліджень і публікацій останніх років. Проблеми безпеки інформаційних систем та методи захисту інформації в цих системах досліджувались у працях багатьох авторів, серед яких: А. І. Марущак [1], Б. А. Кормич [2], Н. В. Гришина [4], С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук [5], К. С. Варивода [6], М. М. Козяр, Я. І. Бедрій, О. В. Станіславчук [8] та ін. Вищевказані автори розглядали основні причини виникнення даної проблеми, вивчали та описували найефективніші методи захисту інформації в інформаційних системах в сучасних умовах.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на наукові доробки з даної тематики, проблеми забезпечення інформаційної безпеки підприємства потребують подальшого вивчення. Актуальним є аналіз особливостей застосування сучасних методів забезпечення безпеки інформації в інформаційних системах.

Мета статті. Метою статті є виділення видів потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій, визначення та аналіз особливостей застосування сучасних методів захисту інформації в інформаційних системах.

Виклад основного матеріалу дослідження. Зі зростанням науково-технічного прогресу зростає і необхідність вирішення проблеми інформаційної безпеки. Інформація – це чинник, який може призвести до технологічних аварій, політичних та військових конфліктів, дезорганізації фінансової системи та державного управління.

Інформаційну безпеку можна визначити, як стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [9].

Поняття інформаційної безпеки стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Для регулювання економічної безпеки на підприємствах створюється служба інформаційної безпеки, яка має виявляти і візуально демонструвати власникам підприємства весь спектр загроз в

інформаційній сфері. Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації [2].

Умисні загрози безпеки інформації діляться на два види:

1) Активні загрози. Вони мають на меті порушення нормального функціонування ІС шляхом впливу на її компоненти. Джерелом таких загроз можуть бути дії взломщиків чи віруси. До активних загроз відносять:

– спотворення відомостей в банках даних;
– виведення з ладу комп'ютера або його операційної системи;
– руйнування програмного забезпечення комп'ютерів, порушення роботи ліній зв'язку.

2) Пасивні загрози. Вони спрямовані на несанкціоноване використання інформаційних ресурсів ІС, не надаючи при цьому впливу на її функціонування. До таких загроз відносять:

– прослуховування каналів зв'язку;
– несанкціонований доступ до баз даних.

Також можемо виділити найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій [3-4]: витік конфіденційної інформації; вільне втручання в програмне забезпечення; компрометація інформації; відсутність регламентованого доступу до файлів даних; несанкціоноване використання інформаційних ресурсів; відсутність протоколювання змін у програмному забезпеченні; помилкове використання інформаційних ресурсів; відсутність дублювання важливих документів на документальних носіях даних; несанкціонований обмін інформацією між абонентами; відсутність регламентації користувачів інформації; відмова від інформації; часті удосконалення одного і того ж програмного забезпечення різними особами; порушення інформаційного обслуговування; наявність непідзвітних посадових осіб у системі управління; незаконне використання привілеїв; відсутність схем інформаційного забезпечення рівнів управління тощо.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися під централізованим управлінням і одночасно. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз [8, с.106].

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які не допускають виток та втрату інформації. Можна виділити декілька основних методів захисту, що активно використовуються підприємцями (табл. 1). Усі перераховані методи ефективно захищають інформацію в інформаційних системах та націлені на побудову ефективної технології захисту інформації, в якій успішно відображено різні види загроз.

Проведене дослідження дає підстави стверджувати, що без належного захисту інформаційного середовища неможливе функціонування підприємства та розвиток його економічної системи.

Таблиця 1

Методи захисту інформації в інформаційних системах
(розроблено на основі [1; 10, 11])

Методи захисту	Особливості
Управління доступом	Методи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи. Ці методи повинні протистояти всім можливим шляхам несанкціонованого доступу до інформації.
Механізми шифрування	Методи криптографічного закриття інформації. Ці методи захисту все ширше застосовуються як при обробці, так і при зберіганні інформації на магнітних носіях. При передачі інформації по каналах зв'язку великої протяжності цей метод є єдино надійним.
Регламентація	Найважливіший метод захисту ІС, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися усі маніпуляції з даними, що охороняються. Передбачає створення таких умов автоматизованої обробки, зберігання та передачі інформації, яка захищається, при яких норми і стандарти цього захисту виконуються в найбільшою мірою.
Примус	Методи захисту інформації, тісно пов'язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила. Користувачі та персонал ІС змушені дотримуватися правил обробки, передачі і використання інформації, що захищається, під загрозою матеріальної, адміністративної чи кримінальної відповідальності.
Маскування	Методи захисту інформації, що передбачають перетворення даних у форму, не придатну для сприйняття сторонніми особами.
Спонукання	Метод захисту, що спонукає користувачів і персонал ІС не порушувати встановлені порядки за рахунок дотримання сформованих моральних і етичних норм.
Перешкода	Метод фізичних перешкод шляху зловмиснику до інформації, що захищається (до апаратури, носіям інформації і т. д.). Розуміється спосіб фізичного захисту ІС, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.
Протидія атакам шкідливих програм	Метод передбачає комплекс різноманітних заходів організаційного характеру і використання антивірусних програм з метою: зменшення ймовірності інфікування АІС, виявлення фактів зараження системи; зменшення наслідків інформаційних інфекцій, локалізація або знищення вірусів; відновлення інформації в ІС.

Висновки з даного дослідження. На основі вищевикладеного матеріалу можемо дійти висновку, що в сучасних умовах інформаційна безпека є надзвичайно важливою складовою системи економічної безпеки будь-якого господарюючого суб'єкта. Адже, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Усі підприємства мають створити добре функціонуючу систему управління інформаційною безпекою, адже це допоможе зберегти капіталовкладення, бізнес, бути конкурентоспроможним та розвиватися.

ЛІТЕРАТУРА

1. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України. 2011. № 21. С. 92–95.

2. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук: [спец.] 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Нац. ун-т внутр. справ. Х., 2004. 42 с.

3. Smieliauskas W., Bewley K. Auditing: An International Approach. Mc-Graw-Hill Ryerson Higher Education, 2006. 800 p.

4. Гришина Н. В. Организация комплексной системы защиты информации. М. : Гелиос АРВ, 2007. 256 с.

5. Гордієнко С. Б., Микитенко О. С., Данильчук В. Г. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії // Вісник ДУІКТ. 2013. № 1. С. 104–107.

6. Варивода К. С. Інформаційна безпека підлітків в Інтернет мережі // Молодий вчений. 2016. № 3. С. 365–368. URL: http://molodyvcheny.in.ua/files/journal/2016/3/85.pdf (дата звернення: 25.03.2019).

7. Варивода К. С. Формування в дітей компетенцій безпечного використання Інтернет-мережі // Журнал науковий огляд. 2015. № 10(20). С. 62–71.

8. Козяр М. М., Бедрій Я. І., Станіславчук О. В. Основи охорони праці, безпеки життєдіяльності та цивільного захисту населення : навч. посіб. К. : Кондор, 2014. 458 с.

9. Інформаційна безпека. URL: https://uk.wikipedia.org/wiki/Інформаційна_безпека (дата звернення: 25.03.2019).

10. Войнаренко М. П., Кузьміна О. М., Янчук Т. В. Інформаційні системи і технології в управлінні організацією : навч. посіб. для студентів ВНЗ. Вінниця : Едельвейс і К, 2015. 496 с.

11. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. Н. Новгород : Изд-во ННГУ, 2006. URL: http://www.iee.unn.ru/wp-content/uploads/sites/9/posobya/ib_yasenev.pdf (дата звернення: 25.03.2019).

12. Фінансово-економічна безпека підприємств та інформаційні технології забезпечення безпеки : монографія / О. В. Орлик, О. О. Кюне, О. Г. Єсіна, А. Ю. Вакула. Одеса : ФОП Гуляєва В.М., 2018. 140 с.

13. Орлик О. В. Інформаційні технології забезпечення безпеки електронного бізнесу // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конференції (Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. С. 167–169.

14. Орлик О. В. Проблеми забезпечення інформаційної складової економічної безпеки сучасних підприємств // Кібербезпека в Україні: правові та організаційні питання : матеріали III Всеукр. наук.-практ. конференції (Одеса, 30 листопада 2018 р.). Одеса : ОДУВС, 2018. С. 79–81.