УДК 002.513

Л. М. Ткачук
О. В. Костюк

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вінницький національний технічний університет

Анотація
Робота присвячена дослідженню основних методів захисту різних видів інформаційних ресурсів в контексті попередження появи загроз втрати або знищення інформації.
Ключові слова: *цифрова безпека, інформаційний простір, шляхи перехоплення інформації, загрози інформаційним ресурсам, способи вирішення проблем несанкціонованого доступу до інформації.*

Abstract
The main purpose of the report consists of studying the main security methods of different information resources in the context of prevention the threat of loss or destruct of information.
Keywords*: digital safety, information area, interception pathways of information, threats to information resources, ways to solve the problem of unauthorized access to information*.

Вступ

У сучасних реаліях, інформація стала одним з найважливіших ресурсів подальшого розвитку чи то підприємства, чи то країни. Повсякденна діяльність будь-якого підприємства, компанії чи країни в цілому, передбачає створення та обмін великою частиною інформаційних ресурсів. На основі вчасно наданої, достовірної і повної інформації приймаються управлінські рішення, тому перед державою стоїть важливе завдання щодо удосконалення процесу та розробка дієвих методик забезпечення захисту інформаційних ресурсів [1, с. 43].

Результати дослідження

Інформаційний ресурс – це власне інформація, або ж те, що є елементом певної інформаційної технології, так звані технічні засоби обчислювальної або телекомунікаційної техніки, програми, дані тощо. Б. Кормич трактує інформаційну безпеку як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб’єктів цих процесів та відносин [2, с. 15]. Деякі вчені розглядають інформаційну безпеку, як стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту та недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [3, с. 72].

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними випадками порушення безпеки інформації можна назвати такі:

− несанкціонований доступ — доступ до інформації, що здійснюється з порушенням правил розмежування доступу;

− витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

− втрата інформації — дія, внаслідок якої інформація перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

− підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися;

− блокування інформації — дії, наслідком яких є припинення доступу до інформації;

− порушення роботи інформаційної системи — дії або обставини, які призводять до спотворення процесу обробки інформації [4].

Такі види порушення цілісності інформаційних ресурсів можуть бути як і з боку людського фактору, так і через збої в інформаційних системах.

Для вирішення, а також попередження виникнення таких проблем використовують такі види захисту інформаційних ресурсів. Кожен вид захисту інформації забезпечує окремі аспекти інформаційної безпеки:

1. Технічний:

− забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

− попередження витоку по технічним каналам;

− попередження блокування ;

2. Інженерний:

− попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

3. Криптографічний:

− попереджує доступ за допомогою математичних перетворень повідомлення (ІП):

− попередження несанкціонованої модифікації ;

− попередження НС розголошення.

4. Організаційний:

− попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу) [5].

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні бути обізнані про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз [6, с. 106].

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз [7].

Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов’язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила.

Коли використовуються способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісним міркувань, то йдеться про спонукання [8].

Висновки

Отже, у сучасних умовах інформаційна безпека є невід’ємною складовою системи економічної безпеки. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Ігнорування хоча б одного з аспектів цієї проблеми може призвести до втрати інформації, яка в житті сучасного суспільства набуває все більш важливого значення і відіграє важливу роль.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Проблеми кібербезпеки [Електронний ресурс]. – Режим доступу: http://fit.univ.kiev.ua/wp-content/uploads/2016/03/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA-%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D1%96%D0%B2-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%97.pdf.

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» / Б. А. Кормич ; Нац. ун-т внутр. справ. — Х., 2004. — 42 с.

3. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. — 2011. — № 21. — С. 92—95.
4. Технології захисту інформації [Електронний ресурс]. – Режим доступу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186 .
5. Захист інформації [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#%D0%92%D0%B8%D0%B4%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.
6. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії / С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. — 2013. — № 1. — С. 104—107.
7. Інформаційна безпека та методи захисту інформації [Електронний ресурс]. – Назва ресурсу: Vznu_eco_2016_1_21.pdf.
8. Ясенев В. Н. Информационная безопасность в экономических системах [Електронний ресурс] — Режим доступу : http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.
Костюк Олег Віталійович – студент групи КІТС-18б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleg.kostuik14@gmail.com.

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.
Kostiuk Oleh Vitaliyovych – student of CITS-18b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: oleg.kostuik14@gmail.com.