УДК 621.391.1

Д. М. Палагнюк
Д. С. Тищук
О. В. Березюк

Принципи забезпечення інформаційної безпеки

Вінницький національний технічний університет

Анотація. *Представлено завдання забезпечення інформаційної безпеки, як одного із головних в сучасному інформаційному суспільстві. Розкрито сутність поняття інформаційної безпеки, основні принципи її забезпечення.*

Ключові слова: *інформація; інформаційна безпека; концепція безпеки; політика інформаційної безпеки; загрози; комп'ютерна система.*

Principles of information security

Abstract. In the article the problem of information security as one of the most important in today's information society. The essence of the concept of information security, *the basic* principles of software.

Keywords: *information; information security; the concept of security; policy information security; threats; computer system.*

Вступ

В новітньому суспільстві основною виробничою силою, найважливішим стратегічним ресурсом, який забезпечує подальший його розвиток, є інформація. Саме тому інформація, як і будь-які інші ресурси, потребує також особливого захисту. Поруч із терміном "захист інформації" широко застосовується термін "інформаційна безпека". Захист інформації характеризує процес створення обставин, які забезпечують потрібну захищеність інформації, а досягнутий стан такого рівня захищеності відображає інформаційна безпека [1].

Питання інформаційної безпеки придбало особливої значущості в новітніх умовах широкого використання інформаційних автоматизованих систем, заснованих на застосуванні комп'ютерних та телекомунікаційних засобів. Під час забезпечення інформаційної безпеки стали абсолютно імовірними загрози, що породжені навмисними (зловмисними) діями громадян. Перші звістки про несанкціонований доступ до інформації пов'язані були, як правило, з хакерами ("електронними розбійниками"). В останнє десятиріччя порушення захисту інформації зростає разом із застосуванням програмних засобів, а також за допомогою мережі Інтернет. Дуже розповсюдженою загрозою інформаційної безпеки також є зараження комп'ютерних систем за допомогою комп'ютерних вірусів.

Отже, у зв'язку із всезростаючою значимістю інформаційних ресурсів у житті новітнього суспільства, а також через імовірності численних загроз з погляду їх захищеності питання інформаційної безпеки потребує більшої і постійної уваги. Системний характер впливу великої сукупності різноманітних обставини на інформаційну безпеку, які мають крім того різну фізичну природу, викликають різні наслідки та переслідують різні цілі, призводять до потреби у системному підході під час вирішення даного питання.

Актуальність дослідження полягає в збільшенні і покращенні інформаційної безпеки та програмного забезпечення.

Результати дослідження

Інформаційна безпека (ІБ) становить собою стан рівня захищеності інформаційного середовища, а захист інформації – це діяльність направлена на запобігання витоку інформації, яка захищається, ненавмисних і несанкціонованих впливів на інформацію, яка захищається, тобто процес, що направлений на досягнення цього стану [2]. Головною метою реалізації ІБ будь-якого об'єкта є реалізація системи забезпечення інформаційної безпеки цього об'єкта.

Усвідомлюючи інформаційну безпеку як "стан рівня захищеності інформаційного середовища суспільства, що забезпечує її формування, розвиток і використання в інтересах організацій та громадян", правомірно встановити загрози безпеки інформації, їхні джерела, способи їхньої реалізації

та мети, інші обставини та дії, що порушують безпеку. Природно, що при цьому потрібно розглядати також заходи захисту інформації від злочинних дій, що спричиняють нанесення збитку.

Під загрозами інформаційній безпеці розуміють можливі події або дії, які можуть вести до порушень ІБ. Різновиди загроз інформаційній безпеці досить різноманітні та мають безліч класифікацій. За різновидом об'єкта впливу загрози поділяються на загрози: власне інформації, діяльності стосовно забезпечення інформаційної безпеки об'єкта та персоналу об'єкта. Після більш детального розгляду загроз інформації, їх можна класифікувати на загрози: носіям конфіденційної інформації, місцям їх розташування (розміщення), системам інформаційного обміну (каналам передачі), а також інформації, що зберігається в електронному (документованому) вигляді на різних носіях інформації.

Один із поширених варіантів класифікації комп'ютерних загроз за характером порушення наведено на рис. 1.

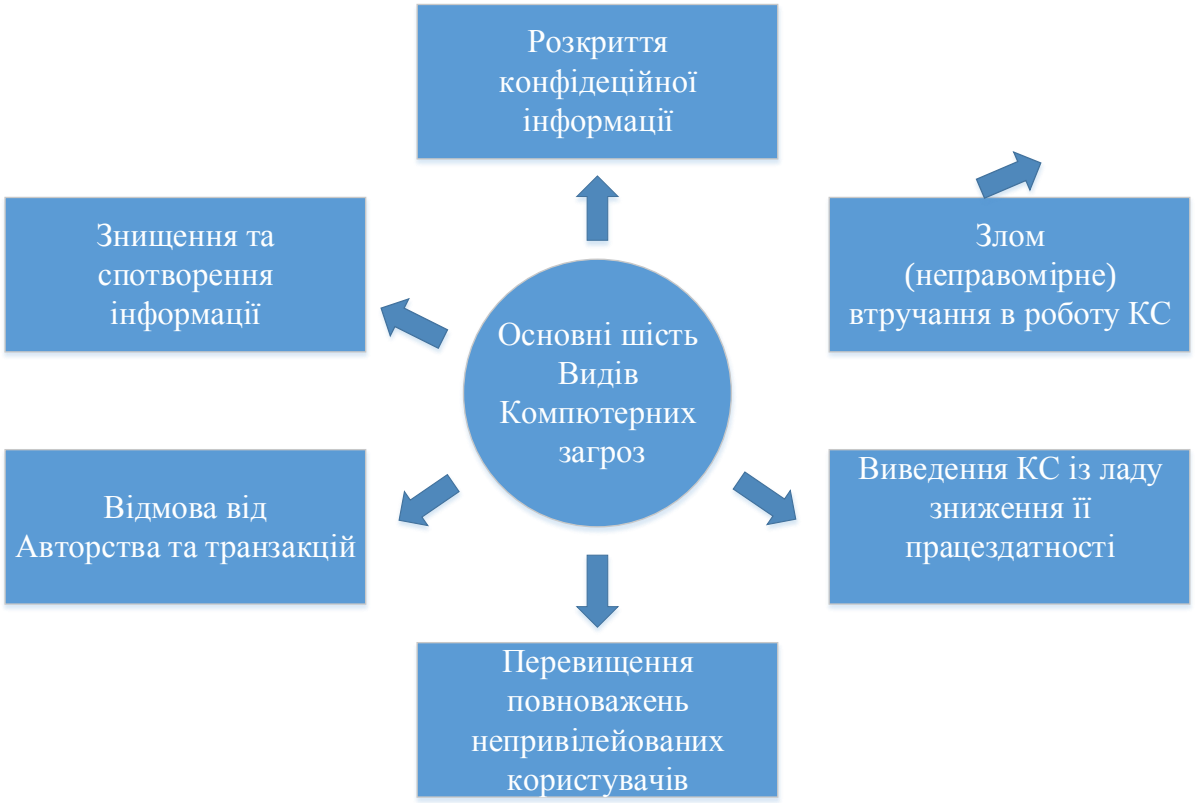

Рисунок 1 – Основні шість видів комп'ютерних загроз

Отже, дію загроз ІБ об'єкта націлено на створення імовірних каналів витоку інформації, яка підлягає захисту, причин її витоку та безпосередньо на витік цієї інформації.

Під час розробки необхідних засобів, заходів і методів, що забезпечують захист інформації, потрібно враховувати велику чисельність різних чинників.

Інформація, як об'єкт захисту, в принципі, може бути представлена на різноманітних технічних носіях. Цими носіями також можуть бути навіть люди з числа обслуговуючого персоналу та користувачів. Інформація може підлягати обробці за допомогою комп'ютерних систем, передаватися за допомогою каналів зв'язку і відображатись різноманітними пристроями. Вона може розрізнятися за своєю значущістю. Об'єктами, які підлягають захисту і в яких може міститись інформація, є не лише комп'ютери та канали зв'язку, але й будівлі, приміщення та прилегла територія. Суттєво може різнитися кваліфікація зловмисників, а також використовувані канали та способи несанкціонованого доступу до інформації.

Прикладом застосування захисту інформації може слугувати захист крипостійкими алгоритмами файлів з тестовими запитаннями і варіантами відповідей, необхідних для проведення перевірки знань студентів шляхом комп'ютерного тестування [3-5].

Отже, головними принципами гарантування інформаційної безпеки є такі [6]:

- комплексності;
- відкритості алгоритмів та механізмів захисту;
- системності;
- простоти застосування захисних заходів та засобів;
- розумної достатності;
- безперервності захисту;
- гнучкості управління та застосування.

Усі заходи гарантування безпеки комп'ютерних систем за способами здійснення поділяють на:
- морально-етичні;
- законодавчі (правові);
- апаратно-програмні;
- фізичні;
- організаційно-адміністративні.

Висновки

Отже, в новітніх реаліях безпека інформаційних ресурсів може бути гарантована лише за допомогою комплексної системи захисту інформації, яка має бути: плановою, безперервною, конкретною, цілеспрямованою, надійною, активною. Система захисту інформації має спиратися на комплекс видів персонального забезпечення, здатного здійснювати її функціонування як в повсякденних обставинах, так і в критичних ситуаціях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту / О. В. Черевко // Ефективна економіка [Електронне наукове фахове видання]. – 2014. – № 5. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=3304.
2. Кавун С. В. Інформаційна безпека : навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків : Вид. ХНЕУ, 2008. – 352 с.
3. Березюк О. В. Комп’ютерна програма для тестової перевірки рівня знань студентів / О. В. Березюк, М. С. Лемешев, І. В. Віштак // Тезиси науково-технічної конференції студентів, магістрів та аспірантів «Інформатика, управління та штучний інтелект», 26-27 листопада 2014 р. – Харків : НТУ «ХПІ», 2014. – С. 7.
4. Березюк О. В. Перспективи тестової комп’ютерної перевірки знань студентів із дисципліни "Безпека життєдіяльності" / О. В. Березюк, М. С. Лемешев, М. А. Томчук // Матеріали дев'ятої міжнародної науково-методичної конференції "Безпека життя і діяльності людини – освіта, наука, практика". – Львів : ЛНУ, 2010. – С. 217-218.
5. Березюк Л. Л. Тестова комп’ютерна перевірка знань студентів із дисципліни «Медична підготовка» / Л. Л. Березюк, О. В. Березюк // Науково-методичні орієнтири професійного розвитку особистості : тези доповідей учасників IV Всеукраїнської науково-методичної конференції, Вінниця, 20 квітня 2016 р. – Вінниця : ТОВ «Меркьюрі–Поділля», 2016. – С. 96-98.
6. Аникин И. В. Теория информационной безопасности и методология защиты информации : учебное пособие / И. В. Аникин, В. И. Глова, Л. И. Нейман, А. Н. Нигматуллина. – Казань : Изд-во Казан. гос. техн. ун-та, 2008. – 358 с.

Палагнюк Дмитро Михайлович – студент групи ТКТ-14б, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця, e-mail: brazers.d29@gmail.com

Тищук Дмитро Сергійович – студент групи ТКТ-14б, факультету інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця, e-mail: dimasboroda96@gmail.com

Березюк Олег Володимирович – кандидат технічних наук, доцент, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: berezyukoleg@i.ua

Palahniuk Dmytro Mikhailovich – student of the group TKT-14b, Faculty infocommunications, electronics and nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: brazers.d29@gmail.com

Tyschuk Dmitry Serhiyovych – student of the group TKT-14b, Faculty infocommunications, electronics and nanosystems, Vinnytsia National Technical University, Vinnytsya, e-mail: dimasboroda96@gmail.com

Bereziuk Oleg Volodymyrovych – Candidate of Technical Sciences (Engineering), Associated Professor, Associated Professor of the Chair Security of Life and Safety Pedagogics, Vinnytsia National Technical University, Vinnytsia, e-mail: berezyukoleg@i.ua