Національна безпека

УДК 351.74/76

Мордвинцев Микола Володимирович
кандидат технічних. наук, доцент,
провідний науковий співробітник науково-дослідної лабораторії
з проблем розвитку інформаційних технологій
Харківський національний університет внутрішніх справ
Мордвинцев Николай Владимирович
кандидат технических наук, доцент,
ведущий научный сотрудник научно-исследовательской лаборатории
по проблемам развития информационных технологий
Харьковский национальный университет внутренних дел
Mordvyntsev Mykola
PhD in Technical Sciences, Leading Researcher of the
Information Technologies Development Problems
Scientific and Research Laboratory
Kharkiv National University of Internal Affairs

Демидов Захар Георгійович
старший науковий співробітник науково-дослідної лабораторії
з проблем розвитку інформаційних технологій
Харківський національний університет внутрішніх справ
Демидов Захар Георгиевич
старший научный сотрудник научно-исследовательской лаборатории
по проблемам развития информационных технологий
Харьковский национальный университет внутренних дел

Demydov Zakhar
Senior Researcher of the Information Technologies Development Problems Scientific and Research Laboratory
Kharkiv National University of Internal Affairs

Колмик Олег Олександрович
науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківський національний університет внутрішніх справ
Колмык Олег Александрович
научный сотрудник научно-исследовательской лаборатории по проблемам развития информационных технологий
Харьковский национальный университет внутренних дел
Kolmyk Oleh
Researcher of the Information Technologies Development Problems Scientific and Research Laboratory
Kharkiv National University of Internal Affairs

ДЕЯКІ СПОСОБИ ЗАХИСТУ КОМП'ЮТЕРНИХ ПРИСТРОЇВ
НЕКОТОРЫЕ СПОСОБЫ ЗАЩИТЫ КОМПЪЮТЕРНЫХ УСТРОЙСТ
SOME METHODS FOR PROTECTING COMPUTER DEVICES

Анотація. *На підставі аналізу темпів розвитку цифрових технологій і широкому їх впровадженні в сучасному інформаційному суспільстві робиться висновок про збільшення злочинів пов'язаних з використанням комп'ютерних технологій. Вироблені деякі рекомендації щодо захисту комп'ютерних пристроїв.*

Ключові слова: *інформаційна безпека, захист комп'ютерів.*

Аннотация. *На основании анализа темпов развития цифровых технологий и широком их внедрении в современном информационном обществе делается вывод об увеличении преступлений связанных с использованием компьютерных технологий. Выработаны некоторые рекомендации по защите компьютерных устройств.*

Ключевые слова: *информационная безопасность, защита компьютеров.*

Summary. *Based on the analysis of the rate of development of digital technologies and their widespread introduction in the modern information society, it is concluded that the crime associated with the use of computer technologies has increased. Some recommendations for protecting computer devices have been developed.*

Key words: *information security, computer protection.*

Вступ. Вагомим фактором, що сприяє швидкому зросту постіндустріальної економіки є інтенсивне впровадження цифрових технологій в самі різні сфери життєдіяльності суспільства. Для реалізації цього у вересні 2019 року було створено Міністерство цифровий трансформації, який планує до 2024 року цифрувати всі публічні державні послуги, навчити близько 6 млн осіб цифровий грамотності та забезпечити 100% покриття високошвидкісним інтернетом. Однак, значна частина населення України перебуває в зоні ризику функціональної неграмотності.

На базі репрезентативна вибірка можна зробити висновок, що це, перш за все, особи старших вікових груп, особи з невисоким рівнем освіти, верстви населення з низькими доходами, мешканці сільської місцевості [1]. Тому дуже важливо включати в програму навчання основні системні положення захисту своїх даних і інформації, яка зберігається на комп'ютері.

Основний матеріал. Існує два види загроз інформаційній безпеці: природні (випадкові) і штучно створені. До природних відносять загрози, що не залежать від людини: пожежа, повінь, землетрус, а також збій або відмова технічних пристосувань, програмні помилки, вихід з ладу пристроїв для зберігання інформації під впливом зовнішніх факторів.

Для цього передбачено резервне копіювання даних (backup). Backup рекомендується здійснювати на зовнішній носій або в «цифровій хмарі», тоді при фізичному знищенні комп'ютера існує можливість відновити інформацію.

При створенні резервних копій необхідно враховувати наступні умови:

- частота створення резервних копій залежить від частоти оновлення інформації;
- зберігати резервні копії на зовнішніх ресурсах з клієнтським шифруванням;
- періодично перевіряти резервні копії на працездатність.

Другий вид загроз інформаційної безпеки - штучні, які, в свою чергу, поділяються на дві групи - випадкові (через незнання, через необережність) і спеціальні (крадіжка і копіювання цифрових документів, несанкціонований доступ до інформації, перехоплення і підробка інформації, хакерські атаки, шифрування даних т. і.).

Розглянемо останню групу загроз - спеціально створені, і способи боротьби з ними.

У будь-якого користувача комп'ютером існують файли, які неможливо відновити, в разі їх знищення. Наприклад, фотографії, документи, особисті відео, власні розробки. Ще існують файли з певним режимом секретності, як на домашньому комп'ютері, так і на робочому – робочі документи, документ з логінами і паролями від різних ресурсів та програм, дані транзакцій по криптовалютам. При ймовірності злому

комп'ютера віддалено або викрадення його фізично, ці файли можуть бути використані в злочинних цілях.

Розглянемо способи захисту інформації від використання в разі викрадення.

Перший спосіб - шифрування даних, наприклад, за допомогою програм VeraCrypt, TrueCrypt і подібних [2; 3]. Приховування файлів, а також папок, в яких вони знаходяться, наприклад, за допомогою програми CyberSafe [4]. При відсутності ключа шифрування у зловмисника немає можливості відкрити файли і визначити ступінь їх цінності.

Другий спосіб - використання апаратних токенів, флеш-накопичувача з паролем. В цьому випадку доступ до комп'ютера або до окремих файлів неможливий без цього носія, навіть якщо зловмисникові відомі логін і пароль користувача.

Третій спосіб - існування декількох паролів, при введенні яких відбувається виконання різних сценаріїв.

Четвертий спосіб - створення складних паролів на месенджерах, папках, аксесуарах, використовувати менеджери паролів (KeyPass), не повторювати паролі і алгоритми їх створення.

Способи захисту необхідно використовувати разом з резервним копіюванням, тоді є велика ймовірність, що навіть при зломі комп'ютера і викраденні файлів або шифруванні даних зловмисник не зможе скористатися цими даними.

Висновок. В період інтенсивної цифровізації економіки країни при масовому навчанні населення комп'ютерній грамотності необхідно велику увагу приділяти способам захисту і зберіганню інформації на особистих комп'ютерах та гаджетах.

Література

1. Баскакова М. Е. Новые грани функциональной неграмотности в условиях цифровой экономики / М. Е. Баскакова, И. В. Соболева // Вопросы образования. Москва: 2019. № 1. С. 244–263.
2. VeraCrypt – инструкции на русском URL: https://veracrypt.ru (дата звернення: 13.05.2021).
3. TrueCrypt. URL: https://truecrypt.ru.uptodown.com/windows (дата звернення: 13.05.2021).
4. Cybersafe. URL: http://cybersafesoft.com/product.php?id=1 (дата звернення: 13.05.2021).