

неимущественные права / Е.А. Суханов. — Москва: Статут, 2011. — 330 с.

УДК 004.056

A.S. Shulgina-Tarachshuk

Karaganda State University named after Academician E.A. Buketova
Karaganada, Kazakhstan

CYBERSECURITY IN THE DIGITAL WORLD

***Abstract.** The article tells about the digital world, which is closely intertwined with our daily life. The rules of behavior on the Internet are considered. Also, the rules for creating strong passwords are considered.*

А.С. Шульгина-Тарашук

Карагандинский университет имени Е.А. Букетова,
Караганда, Казахстан

КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОМ МИРЕ

***Аннотация.** В статье рассказывается о цифровом мире, который тесно сплелся с нашей повседневной жизнью. Рассматриваются правила поведения в Сети. А также рассмотрены правила создания надежных паролей.*

The digital world is closely intertwined with our daily life: we communicate for a long time, study, work, shop online [1].

First of all, one must clearly understand the scale of a possible tragedy. Many people are reckless about internet safety. So, here's what hackers can find out about you by gaining access to your phone or computer:

- Photos, videos and other content (even if it is stored in the cloud).
- Information about documents: passport, policy, tickets and others. This is especially true if you store digital copies of them in applications such as "VKarmane", Wallet, or even in the "Photos" folder.
- Financial information, including your card CVV, account movements, recent payments.
- Everything that happens in all your social networks (hacking of the VKontakte account, by the way, is one of the top most expensive hacker services) and mail, access to attachments in messages and confidential corporate and personal correspondence.

- Geolocation, microphone and camera data.

A compromised or weak password is the second most popular hacking method (according to a study by Balabit). Nevertheless, from year to year, in the lists of the most popular passwords, we can see the classic qwerty, 12345, or even just password. The opposite situation happens: a person comes up with a super-long and complex password and uses it in all his accounts: social networks, forums, online stores, personal bank accounts. Now, when each of us is registered in at least ten different online services, a single password becomes the key to a person's entire life and can greatly harm it. Preventive measures:

- Determine the complexity of the password based on which account it leads to. Obviously, the security of an Internet bank is more important than an account on an amateur forum.

- A strong password consists of at least eight characters and meets the following requirements: the presence of upper and lower case letters (agRZhtj), special characters (!% @# \$? *) And numbers. There are 814 trillion (!) Brute-force combinations for a 14-character password. To check how long it will take for hackers to crack your password, visit howsecureismypassword.net.

- Do not use common words or personal information that is easily obtained from open sources: birthdays, pet names, company or university name, your nickname, and the like. For example, the password is 19081091, where 1991 is the year of birth, and 0810 is the date and month, not as reliable as it seems at first glance. You can write the title of your favorite song or a line from a poem in a different layout. For example, Tchaikovsky Swan Lake → XfqrjdcrbqKt, tlbyjtjpthj.

- Protect critical services with one-time passwords. To do this, you can download the manager apps that generate them, such as KeePass and 1Password. Or use two-factor authentication, when each login to your account will need to be confirmed with a one-time SMS code.

A wide public Wi-Fi network helps residents of large cities to reduce their mobile Internet costs. Nowadays, it's rare to find a place without a Free Wi-Fi badge. Public transport, parks, shops, cafes, beauty salons and other urban spaces have long provided their visitors with free internet. But even in your favorite trusted place, you can run into a hacker.

Since the personal data of almost any of us is entrusted to information systems, social networks, mobile applications, digital devices, everyone needs to know the basics of cybersecurity. As for the developed European countries (for example, Great Britain), today training of this type is carried out there already from the school bench. In particular, young citizens are taught skills that

will help protect their organization from online hacker attacks in the future. These are both online lessons and extracurricular activities. It is also supposed to discuss current cybersecurity problems with students, independently look for ways to solve them.

There are no such initiatives in our country yet. However, it is worth hoping that citizens who are equally involved in virtual reality with the whole world will soon begin to worry about the safety of their own data, and cybersecurity courses will also become relevant in our country.

Список использованных источников:

1. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 - Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. - М.: ГЛТ, 2017. - 536 с.

УДК 33.004

М.С. Кулинкович, А.К. Крамаренко

Брестский государственный технический университет,
г. Брест

ОСОБЕННОСТИ ИТ ОБЕСПЕЧЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. В докладе рассмотрены различные данные и системы, определяющие уровень внедрения информационных технологий в бизнесе Беларуси, а также выявлена их ключевая роль в предпринимательской деятельности.

M.S. Kulinkovich, A.K. Kramarenko

Brest state technical university,
Brest

FEATURES OF IT SUPPORT OF ENTREPRENEURIAL ACTIVITIES IN THE CONDITIONS OF THE DIGITAL ECONOMY

Abstract. The report examines various data and systems that determine the level of implementation of information technologies in business in Belarus, and also identifies their key role in entrepreneurial activity.