**Forum:** Special Conference

**Issue:** Ensuring the right for personal data protection, privacy, and the secrecy of correspondence in the Information Age

**Student officers:** Alisa Balybina, Daria Leus

## Introduction

The Internet has become an integral part of our lives. It allows people to communicate with each other despite the distance between them, shop online, share ideas with the public and capture moments through photos and music. The Internet has a huge number of advantages, and it makes our lives easier. However, it can be dangerous in terms of possible theft of personal data. Now this problem is more important than ever before and, therefore, it is so essential to protect people's privacy, and the secrecy of correspondence in the Information Age.

Identity theft or theft of personal data is a type of fraud, which results in the theft of personal information, such as passwords, user names, Bank data, credit card numbers, etc. This crime is widespread on the Internet. Attackers often use phishing attacks to steal personal information.

The researchers identify several groups of property that is most often subject to theft. They are the parameters of access to financial systems, to Internet pagers and websites, e-mail addresses, passwords to online games. For the implementation of theft most often used by malicious programs or methods of social engineering.

Violation of the rights of people to inviolability of correspondence and private life is widespread on the Internet. People obtain information illegally, for example, by hacking into a social network, and getting an opportunity to threaten their victims with dissemination of this information. Criminals can extort money or demand the performance of any actions beneficial to them. These offences have a negative impact on people due to the strongest moral harm caused by them.

Millions of people suffer from identity theft every year. According to Harris Poll, approximately 60 million Americans were affected by identity theft in 2017. It is also noted that slightly less than two-thirds of adult survey participants said they had never checked their credit card statements, although monitoring a credit card report could help them protect their finances from theft. According to Identity Theft Resource Center (ITRC), there were 1,579 data leaks in 2017, affecting approximately 179 million records.

The biggest data breach was the case of Equifax, one of the three major credit reporting agencies. The victims were about 147.9 million people, and, therefore, the amount of compromised data is huge. The stolen information contained names, dates of birth, addresses, and insurance numbers. One of the most high-profile data loss incidents was the incident with Uber in 2016. Hackers stole data on 57 million Uber customers, and the company paid $ 100,000 to hide the theft. Obviously, the risk of identity theft is very high, and it is unlikely that it will decrease in the near future. That is why it is necessary to try to protect people from crimes.

Another important aspect of the issue is the problem of balance between national security and the secrecy of correspondence. Nowadays a lot of people use different messengers that encrypt their data and keep it safe and secure. Unfortunately, the same messengers may be used by the organized criminal groups, drug dealers, or terrorists, and this is the case why governments in different countries may be alarmed by the massive usage of encrypting messengers and may look for ways of monitoring this sphere. This is why there may be a serious tension between the right for privacy and the interests of national security.

**Definition of key terms**

Personal data - any information that relates to an identified or identifiable living individual; different pieces of information, which collected together can lead to the identification of a particular person.

Privacy - the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively; the boundaries and content of what is considered private differ among cultures and individuals, but share common themes: when something is private to a person, it usually means that something is

inherently special or sensitive to them; the domain of privacy partially overlaps with security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.

Secrecy of correspondence – originally a fundamental legal principle that guarantees that the content of sealed letters is never revealed and letters in transit are not opened by government officials or any other third party. Now it is expanded to new types of communication, such as social networks or messengers.

The Information Age (also known as the Computer Age, Digital Age, or New Media Age) - a historic period in the 21st century characterized by the rapid shift from traditional industry that the Industrial Revolution brought through industrialization, to an economy based on information technology.

Identity theft - the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

Phishing - the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

**Background information**

Identity theft is divided into several types. One of the most common of these is the theft of financial personal data. This type of crime began to spread a few years ago with the development of online shopping and banking. The second type is medical identity theft. The crime is that the person steals your health insurance data to get medical care. After the thief uses your health insurance, doctors can update your records with the medical details of the impostor. This can lead to you completing some treatment and having to pay for it. In 2016 alone, US medical records were stolen 9 times more (27 million) than financial records. There is a theft of personal data on employment. This type is very common in Europe. With this kind of theft, criminals are trying to avoid paying taxes. A new type of identity theft is known as synthetic identity theft, which involves fraudsters combining fabricated and real data to create a false identity. This type is often

used to take out a loan or get a credit card. Thus, crimes related to the theft of privacy, and the secret of correspondence appeared a few years ago and now they are at the peak of prevalence.

Current situation

In January-March 2018, the number of leaks of confidential information increased compared to the same period last year. Theft of personal data turns into a permanent business for many hacker groups: obtained by dishonest information attackers sell in the darknet.

At the beginning of the year, Indian journalists reported about the compromise of personal data of more than a billion people, according to the analytical center InfoWatch.

The prey of hackers at the end of February was the information of 150 million people using the application for weight loss MyFitnessPal. Email addresses, logins and encrypted passwords of subscribers were stolen.

The information bomb was the compromise of data of 50 million Facebook users. Facebook says at least 50 million users' data were confirmed at risk after attackers exploited a vulnerability that allowed them access to personal data. The company also preventively secure 40 million additional accounts out of an abundance of caution. Facebook CEO Mark Zuckerberg said that the attackers were using Facebook developer APIs to obtain some information, like "name, gender, and hometowns" that's linked to a user's profile page. The vulnerability was introduced on the site in July 2017, but Facebook did not know about it until September 16, 2018, when it spotted a spike in unusual activity. That means the hackers could have had access to user data for a long time, as Facebook is not sure right now when the attack began.

Ukrainian security researcher found two databases on the network containing information about more than 18.5 million customers of the postal service, that is more than 40% of the population of the Republic. Experts warn that such information can be used not only to send spam, but also as a basis for phishing attacks.

The leakage of medical data of about 3 million citizens of Norway occurred as a result of a hacker attack on the information system of the South-Eastern health service.

The shown crimes related to personal information were the largest and most discussed in 2018.

**Related information and documents**

The study: UN TRADE AND DEVELOPMENT - Data protection regulations and international data flows

The study gives very detailed information on the subject of data protection, including the key challenges, global development, regional initiatives, national experience and other related aspects.

Convention on Human Rights and Biomedicine

Personal health data is one of the most sensitive personal data. The protection of privacy and personal data is, therefore, regulated in Article 10 of the Convention on Human Rights and Biomedicine (ETS No 164) and Article 16 of the Additional Protocol to this Convention concerning Genetic Testing for Health Purposes (CETS No 203).

EU Data Protection Directive 95/46

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data took up, in greater detail, the principles contained in Convention No. 108.

However, it offers improved protection rules on a variety of points. It has established criteria for making data processing legitimate. The catalogue of the data subject's rights has been extended. Right of access includes the right to know the source of the data and the logic used to process them. The directive establishes the right to object to processing of personal data and the right not to be subject to wholly automated decisions. In addition, the controller is required to give certain information to the data subject. Currently, the EU data protection law is undergoing a reform.

Article: Privacy and Data Protection in an International Perspective (by Lee A. Bygrave)

A review of the development of regulatory instruments (statutes, recommendations, guidelines, etc.) to protect privacy and related interests with regard to the processing of personal data.

**Useful links and resources**

https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

https://www.wired.com/story/how-facebook-hackers-compromised-30-million-accounts/

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

https://en.wikipedia.org/wiki/Secrecy_of_correspondence