International Scientific and Practical Conference
"Informatics: Problems, Methods, Technologies" (IPMT)

Confidentiality in cyberspace and how it is violated

A. A. Ganiev
K. F. Kerimov
Z. I. Azizova

Abstract:

Cyberspace is a new platform for social activities. Necessity to develop and improve legal restrictions on access to users' private information is as urgent as development and improvement of methods, mechanisms and software tools to protect personal data in cyberspace. This article discusses ways to breach privacy in cyberspace, as well as the application of personal data de-identification as a data privacy method.

Keywords:

personal data, cyberspace, privacy breach, data compromise, global network, de-identification.

Introduction

Nowadays, there are a number of international and national legislations that limit the collection and use of personal data in cyberspace, ensuring the privacy of personal data of users, based on the idea of "fair information practices" as a necessity to develop the concept of multidimensional privacy on the Internet. Along with the protection of personal data, the process of de-identification of personal data becomes a necessary condition for the process of digitalization of society.

De-identification is a good strategy to preserve the usefulness of personal data and to reduce the risks of its compromise afterwards. When a dataset has undergone a de-identification process and it is not possible to determine whether the individual data belongs to a specific data subject, the data protection law becomes null and void. In this case, creating a true anonymised dataset from a huge set of personal data, with only the required information retained, becomes a difficult task.

Fields of attack targeting the dissemination of confidential information in cyberspace

Information processing and sharing are becoming a major revenue stream for many organizations. Improvements in Internet capabilities, such as increased speed and reduced costs of use, have given the global network a role to play. Focusing on key principles (obligations limiting the use of personal data; open and transparent data processing systems; limited procedural and substantive rights; timely external controls) "fair information practices« provides the basis for modern international legislation on personal data protection and privacy. Consequently, each new improvement in the performance of the technical infrastructure and the connection of each new user to the global network has a positive effect on those who are already active users in cyberspace. Because cyberspace can be organized in any way, it is possible to create highly effective conditions for the security of privacy in cyberspace. This is facilitated by the various technical components and software tools that are used for the lawful use of personal data in cyberspace.

According to the Positive Technologies report "Topical Cyber Threats: Q1-2022" [3] in the first quarter of 2022, the number of detected attacks increased by 14.8% over the fourth quarter of 2021 to 714 detected attacks. At the same time, attacks against individuals accounted for 15% of the total number of detected attacks in Q1-2022. Thus, out of 107 detected attacks on individuals 49 attacks resulted in stealing user credentials, 22 attacks resulted in compromising payment card data, 20 attacks compromised personal data, 3 attacks resulted in providing correspondence data of individuals and 11 attacks resulted in compromising other information.

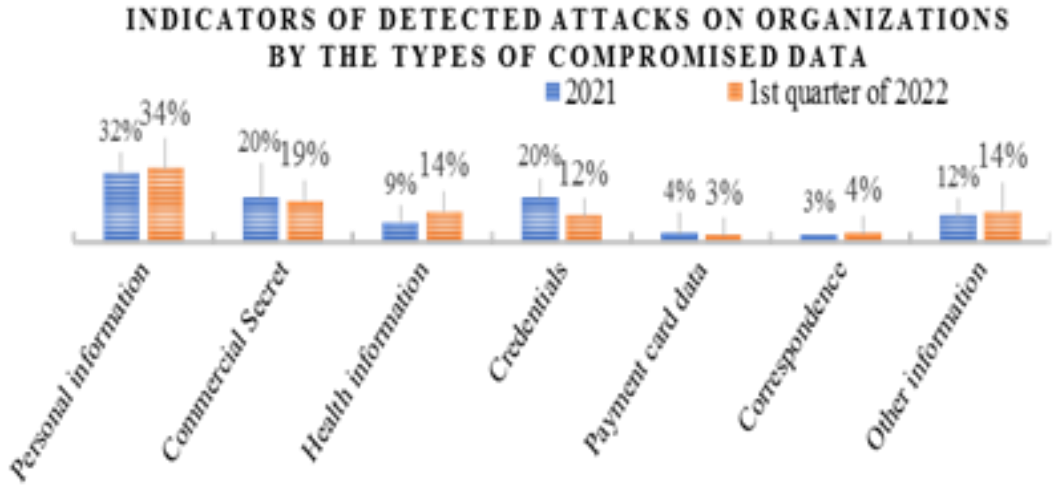

Fig. 1. Data theft rates in attacks on organisations

It should be noted that cybercriminals predominantly targeted personal data belonging to employees of organizational structures. When comparing this indicator to the types of stolen data for 2021, we can observe an upward trend of 2%. Fig. 1 illustrates this point.
Thus, we can conclude that the number of realized attacks on individuals is increasing, as well as the interest of attackers to sensitive user data, in particular personal data used by cybercriminals as a consequence of this, should be carried out to carefully select the tools and methods used to protect sensitive data.

In each of the aforementioned areas a certain amount of detailed personal data emerges, and often cyberspace users falsely believe that they can control the process of personal information distribution - to limit this or that level of anonymity online, or to provide the data they publish with full disclosure of their identity and preferences. In reality, most users have no control over the complex processes of creating, integrating and publishing personal data, or no idea about the subsequent use of the data they publish online.

The protection of personal data covers not only the definition of measures and means of personal data protection, but also the reduction of cost indicators allocated to data protection while complying with basic information protection requirements; training of personal data operators and compliance with the rights of subjects in the search, data collection and data processing of personal data in information systems. In this work, statistical indicators were analyzed in terms of the most relevant areas for data retrieval by attackers.

THANK YOU FOR ATTENTION!