Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs
Yakymenko Danylo Kostiantynovych
cadet of the faculty of training specialists for criminal police units of Donetsk State University of Internal Affairs

CRYPTOGRAPHIC PROTECTION OF INFORMATION IN INFORMATION SUBSYSTEMS

Cryptography is a technique used to protect information in information systems. It involves the use of mathematical algorithms and protocols to ensure the confidentiality, integrity, and authenticity of data. Cryptographic protection is used to prevent unauthorized access, modification, or disclosure of sensitive information.

There are various cryptographic techniques that can be used to protect information in information subsystems, including:

Encryption: Encryption is the process of converting plaintext into ciphertext to protect it from unauthorized access. The ciphertext can only be deciphered using a key or password. Encryption can be used to protect data both in transit and at rest.

Hashing: Hashing is a technique that converts data of any length into a fixed-size output called a hash value. The hash value is unique to the data and can be used to verify the integrity of the data. Hashing is often used to protect passwords and other sensitive data.

Digital signatures: Digital signatures are used to verify the authenticity and integrity of data. A digital signature is a mathematical algorithm that creates a unique digital fingerprint of data. This fingerprint is then encrypted using the sender's private key, which can be decrypted using the sender's public key. Digital signatures are often used to protect email messages and electronic documents.

Key management: Key management is the process of generating, storing, distributing, and revoking cryptographic keys. Cryptographic keys are used to encrypt and decrypt data and must be protected to ensure the security of the system.

Cryptography is used to protect information in information systems, including those used by the National Police of Ukraine.

here is some additional information about cryptographic protection of information in information subsystems used by the National Police of Ukraine.

Secure Communication Channels: The National Police of Ukraine uses secure communication channels, such as virtual private networks (VPNs) and secure sockets layer (SSL) protocols, to protect sensitive information that is transmitted over networks.

Physical Security: The National Police of Ukraine also implements physical security measures to protect its information subsystems, such as access control systems, video surveillance, and secure storage facilities.

Key Escrow: The National Police of Ukraine uses key escrow to ensure that encryption keys can be recovered in case of a lost or forgotten key, or a change in personnel. Key escrow involves storing a copy of the encryption key with a trusted

third-party, such as a secure key management service provider.

Access Control: The National Police of Ukraine uses access control measures to limit access to its information subsystems to authorized personnel only. This includes using strong passwords, two-factor authentication, and role-based access control.

Data Backup and Recovery: The National Police of Ukraine regularly backs up its sensitive data and implements disaster recovery plans to ensure that critical information can be quickly restored in case of a system failure or other disaster.

Cybersecurity Training: The National Police of Ukraine provides cybersecurity training to its personnel to ensure that they are aware of the latest threats and best practices for protecting sensitive information. This includes training on safe handling of encryption keys and digital signatures, as well as identifying and reporting security incidents.

Audit and Monitoring: The National Police of Ukraine conducts regular audits and monitoring of its information subsystems to ensure compliance with policies and regulations, as well as to identify and respond to security incidents in a timely manner.

Overall, the National Police of Ukraine takes a holistic approach to cryptographic protection of information in its information subsystems, including implementing technical measures, establishing policies and procedures, conducting regular assessments, and providing training to personnel. This helps to ensure the confidentiality, integrity, and availability of sensitive information and prevent unauthorized access and disclosure.

Афанас'єва Дар'я Дмитрівна
курсантка 3-го курсу факультету підготовки фахівців для підрозділів досудового розслідування Донецького державного університету внутрішніх справ, рядова поліції
науковий керівник: Крушиницький Андрій Васильович
т.в.о. завідувача кафедри кримінального процесу та криміналістики факультету підготовки фахівців для підрозділів досудового розслідування Донецького державного університету внутрішніх справ, капітан поліції

ДО ПИТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Перш за все слід зазначити, що сьогодні інформаційна-аналітична діяльність правоохоронних органів, зокрема оперативних підрозділів Національної поліції України безсумнівно мають стратегічне значення. Від певної якості та кількості оперативно значущої інформації залежить ефективність усього комплексу виконаних заходів, спрямованих на вирішення поставлених завдань із протидії злочинності. Проте варто зауважити що організація інформаційно-аналітичного забезпечення правоохоронних органів і використання його можливостей ефективні тільки за умов адекватного правового регулювання цієї діяльності. Застосування сучасних інформаційних