УДК 004.056:355

ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Д.Г. Муравицкий, В.А. Федоренко
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматриваются особенности обеспечения информационной безопасности в условиях проведения специальной военной операции. Анализируются основные угрозы информационным системам и каналам связи, возникающие при активном применении средств радиоэлектронной борьбы, разведки и информационно-психологического воздействия. Рассматриваются технические и организационные меры защиты информации, направленные на сохранение конфиденциальности, целостности и доступности данных. Особое внимание уделяется применению криптографической защиты, защищенных каналов связи, а также мерам противодействия утечкам информации в современных условиях ведения боевых действий.

Ключевые слова: защита информации; информационная безопасность; радиоэлектронная борьба; криптографическая защита; каналы связи; военные информационные системы; утечка информации; кибербезопасность; средства защиты информации; информационные угрозы.

INFORMATION SECURITY DURING A SPECIAL MILITARY OPERATION

D.G. Muravitski, V.A. Fedorenko,
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The paper considers the features of ensuring information security during a special military operation. The main threats to information systems and communication channels that arise during the active use of electronic warfare systems, intelligence tools and information-psychological operations are analyzed. Technical and organizational measures aimed at protecting information and maintaining the confidentiality, integrity and availability of data are considered. Particular attention is paid to the use of cryptographic protection, secure communication channels and measures to prevent information leakage in modern combat conditions.

Keywords: information security; electronic warfare; cryptographic protection; communication channels; military information systems; information leakage; cybersecurity; information protection technologies; electronic countermeasures; secure communication.

Введение

Современные вооруженные конфликты характеризуются активным применением информационных технологий и средств радиоэлектронной борьбы. В условиях специальной военной операции (СВО) защита информации становится ключевым фактором устойчивости управления войсками и сохранения боеспособности подразделений.

Информационные системы военного назначения обеспечивают передачу команд, управление вооружением и взаимодействие подразделений. Нарушение их функционирования может привести к потере управления, утечке секретных сведений и снижению эффективности действий войск.

В связи с этим особую актуальность приобретает внедрение комплексных мер защиты информации, направленных на предотвращение несанкционированного доступа, перехвата данных и воздействия средств РЭБ.

Основная часть

В ходе проведения специальной военной операции информационные системы и каналы связи подвергаются следующим основным угрозам: радиоэлектронное подавление подразделениями РЭБ; перехват и анализ радиопереговоров средствами радиоразведки; утечка информации через персональные устройства военнослужащих.

Широко применяются методы киберразведки, включая OSINT, социальную инженерию и анализ данных из социальных сетей. Противник осуществляет мониторинг мессенджеров, отслеживание геолокации и анализ метаданных фото- и видеоматериалов, что позволяет выявлять расположение и характер деятельности подразделений. Особую уязвимость представляет использование личных мобильных устройств, которые передают геоданные, подключаются к небезопасным сетям и могут содержать вредоносное ПО. Человеческий фактор становится причиной более 60% утечек информации.

Защиту информации обеспечивают подразделения связи, РЭБ и группы кибербезопасности. Подразделения связи развертывают защищенные каналы, РЭБ подавляют средства связи противника и защищают собственные каналы, а мобильные группы кибербезопасности ведут мониторинг цифровой активности и предотвращают утечки. Применяются криптографические методы: симметричные алгоритмы

(AES), асимметричные (RSA, ECC) и защищенные мессенджеры со сквозным шифрованием.

Технические меры включают использование экранирующих средств (мешки Фарадея) и технологию псевдослучайной перестройки рабочей частоты (ППРЧ), затрудняющую обнаружение и подавление сигналов. Организационные меры предусматривают инструктаж по информационной безопасности, запрет на использование личных устройств в зоне боевых действий и обучение личного состава основам цифровой гигиены, включая распознавание фишинга и методов социальной инженерии. Особое внимание уделяется контролю за использованием мобильных устройств и соблюдению правил защиты информации.

Комплексное применение технических, организационных и образовательных мер позволяет повысить устойчивость систем управления войсками и снизить вероятность утечки информации в условиях активного противодействия противника. Эффективность защиты информации напрямую зависит от согласованности действий подразделений связи, РЭБ и кибербезопасности, а также от уровня подготовки личного состава. Реализация комплексного подхода к защите информации обеспечивает устойчивость управления войсками и сохранение боеспособности подразделений при ведении современной войны.

Заключение

Таким образом, защита информации в условиях проведения специальной военной операции является важнейшим элементом обеспечения эффективности управления войсками. Активное применение противником средств радиоэлектронной борьбы и кибератак требует использования современных технологий информационной безопасности.

Повышение защищенности информационных систем достигается за счет применения криптографической защиты, защищенных каналов связи, распределенных систем передачи данных и строгих организационных мер безопасности. Реализация комплексного подхода к защите информации обеспечивает устойчивое функционирование систем управления и повышения эффективности действий подразделений в современных условиях боевых действий.

Список использованных источников

1. Манойло А. В. Фейки: траектория лжи. Информационный фронт специальной военной операции / А. В. Манойло, А. И. Петренко, Б. А. Рожин, К. С. Стригунов. – Москва : Горячая линия – Телеком, 2023. – 272 с.

2. Смирнов С. В. Криптографические методы защиты информации / С. В. Смирнов. – Санкт-Петербург : БХВ-Петербург, 2021. – 312 с.

3. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th ed. – London : Pearson, 2017. – 766 p.

References

1. Manoylo A.V., Petrenko A.I., Rozhin B.A., Strigunov K.S. Fakes: Trajectory of Lies. Information Front of the Special Military Operation. Moscow: Goryachaya liniya – Telekom, 2023. 272 p.

2. Smirnov S.V. Cryptographic Methods of Information Protection. St. Petersburg: BHV-Petersburg, 2021. 312 p. (in Russian)

3. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. London: Pearson, 2017. 766 p.

Сведения об авторах

Муравицкий Д.Г., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danikmuravitskiy@mail.ru

Федоренко В.А., начальник цикла кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.fedorenko@bsuir.by

Information about the authors

Muravitski D.G., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", danikmuravitskiy@mail.ru

Fedorenko V.A., Head of the cycle of the Department of Communications, Educational Institution "Belarusian State University of Informatics and Radioelectronics", v.fedorenko@bsuir.by