УДК 355.237

Демьянков Андрей Алексеевич,
преподаватель
Юркевич Артур Дмитриевич,
студент 2 курса
Белорусский государственный университет
г. Минск, Республика Беларусь

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ

Аннотация. В статье исследуются основные элементы обеспечения информационной безопасности в Республике Беларусь с учетом современных вызовов и тенденций, обусловленных цифровизацией. Рассматриваются текущее состояние системы информационной безопасности и современные угрозы. В этой связи особое внимание уделяется рассмотрению ключевых нормативных правовых основ, упорядочивающие общественные отношения в данной сфере. Сделаны выводы о перспективных направлениях подготовки военных специалистов в сфере информационной безопасности.

Ключевые слова: информационная безопасность, цифровизация, киберугрозы, военное образование, военная педагогика.

Abstract. The article examines the main elements of ensuring information security in the Republic of Belarus, taking into account modern challenges and trends caused by digitalization. The current state of the information security system and modern threats are considered. In this regard, special attention is paid to the consideration of key regulatory legal frameworks that regulate public relations in this area. Conclusions are drawn about promising areas of training for military specialists in the field of information security.

Keywords: information security, digitalization, cyber threats, military education, military pedagogy.

В последние десятилетия наблюдается стремительный рост научно-технического потенциала, особенно в тех областях, которые представляются критически важными для обеспечения обороноспособности и национальной безопасности. В связи с глобальной цифровизацией одной из важнейшей составляющей национальной безопасности как Республики Беларусь, так и других государств, является информационная безопасность.

Следует отметить, что на сегодняшний день в Республике Беларусь функционирует комплексная система поддержания информационной безопасности. Среди ее ключевых элементов следует отметить нормативное регулирование, деятельность органов государственного управления, направленных на ее обеспечение, механизмы межведомственного взаимодействия и между-

народного сотрудничества в сфере кибербезопасности, а также систему технических и программных средств защиты информации.

Согласно Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, информационная безопасность представляет собой состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. При разработке данного правового акта программного характера были учтены и в последующем закреплены основные стратегические задачи и приоритеты в области обеспечения информационной безопасности. Кроме того, в Концепции национальной безопасности, утвержденной решением Всебелорусского народного собрания от 25 апреля 2024 г. № 5 [2], обозначены меры, направленные на противодействие внешним и внутренним угрозам национальной безопасности в информационной сфере, которые в настоящее время успешно реализуются на практике.

По нашему мнению, в основе надлежащей охраны рассматриваемой составляющей национальной безопасности является, в первую очередь, комплексное регулирование общественных отношений в информационной сфере. Так, применительно к правовому регулированию, наряду с программными документами, следует отметить детализированную регламентацию указанных выше общественных отношений на уровне законодательных актов, к числу которых относятся Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [3] (упорядочивающий общественные отношения в информационной сфере, в том числе порядок использования информационных технологий), Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [4] (предусматривающий правила и основания обработки персональных данных, их защиту) и др.

Вместе с тем, увеличение возможностей, предоставляемых современными информационно-коммуникационными технологиями, пропорционально увеличивает и потенциал общественно опасных деяний, совершаемых в цифровом пространстве, которые направлены на причинение вреда объектам, наиболее значимым в сфере государственной и общественной жизни. Сегодня многие преступления стали совершаться с использованием информационно-коммуникационных технологий, а киберпреступления и вовсе стали совершаться практически ежедневно. Основу регламентации ответственности за совершение общественно опасных и общественно вредных деяний, охватывающих и вредоносные «кибердеяния», составляют соответственно Уголовный кодекс Республики Беларусь [5] и Кодекс Республики Беларусь об административных правонарушениях [6]. Одним из важных признаков киберпреступлений является их трансграничный характер, т. е. территория их совершения может не ограничиваться политико-географическими рамками одного государства, в связи с чем существенно усложняется механизм борьбы с данными деяниями.

В свою очередь на национальном уровне разработаны практические основы борьбы с киберпреступлениями. Кроме того, как отметил 26 февраля 2025 г. Генеральный прокурор Республики Беларусь А. И. Швед, сегодня реализуется план дополнительных мер по противодействию киберпреступлениям, в том числе уже используется автоматизированная система обработки инцидентов Национального банка Республики Беларусь, что позволяет минимизировать мошенничества с использованием информационно-коммуникационных технологий [7]. Одним из важнейших направлений в этой связи является и организация обучения, подготовки кадров различных ведомств и служб для грамотного выявления, пресечения и профилактики киберправонарушений, что также нашло отражение в Комплексном плане мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2024 – 2025 годы [8].

В условиях повсеместного внедрения информационно-коммуникационных технологий во все ключевые сферы деятельности сегодня к числу приоритетных направлений безусловно, относятся: совершенствование технологий хранения и обеспечения защиты передачи информации, в том числе трансграничной, автоматизация командно-штабных и боевых процессов, цифровизация систем государственного и военного управления, а также военно-экономической и социальной инфраструктуры.

Принимая во внимание указанное выше, среди актуальных аспектов военной педагогики в Республике Беларусь следует обозначить проведение комплексного обучения, направленного на подготовку высококвалифицированных специалистов в области информационной безопасности. В данной связи представляется возможным отметить следующие перспективные направления обучения военных в контексте новейших информационных и технологических вызовов и угроз:

1) освоение нормативных основ регулирования общественных отношений, складывающихся в сфере или по поводу информационной безопасности;

2) формирование междисциплинарных компетенций, сочетающих знания в области кибербезопасности, криптографии, психологической устойчивости и оперативной аналитики;

3) обучение механизмам противодействия использования технологий искусственного интеллекта в противоправных целях;

4) внедрение симуляционных и тренажерных комплексов, имитирующих киберугрозы и информационные атаки, для формирования навыков их своевременного преодоления;

5) повышение уровня цифровой грамотности среди военнослужащих и устойчивости к информационному воздействию;

6) участие в обмене опытом с представителями правоохранительных и военизированных структур государств – участников Содружества Независимых Государств в сфере кибероборонны.

Реализация образовательных программ, в том числе в рамках повышения квалификации и переподготовки, которые будут системно включать данные направления, позволит обеспечивать информационную безопасность и компетентно противостоять возникающим угрозам.

Таким образом, система обеспечения информационной безопасности в Республике Беларусь демонстрирует устойчивое развитие и адаптацию к современным вызовам. Однако в условиях цифровизации и цифровой трансформации угроз требуется постоянное совершенствование практических механизмов противодействия данным негативным явлениям. Ключевым элементом эффективной защиты информационного пространства остается подготовка квалифицированных военных специалистов, способных действовать в условиях информационного противоборства. Формирование новых подходов в военной педагогике и интеграция цифровых компетенций в систему военного образования составляет важнейшую задачу современного этапа развития белорусского государства.

Список использованных источников

1. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 // ilex : информ : правовая система. – Дата доступа: 25.03.2025.

2. Концепция национальной безопасности Республики Беларусь : решение Всебелорус. нар. собр. от 25 апр. 2024 г. № 5 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P924v0005. – Дата доступа: 25.03.2025.

3. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З : в ред. от 10 октября 2022 г. № 209-З // ilex : информ : правовая система. – Дата доступа: 25.03.2025.

4. О защите персональных данных [Электронный ресурс]: Закон Респ. Беларусь от 7 мая 2021 г. № 99-З : в ред. от 1 июня 2022 г. № 175-З // ilex : информ : правовая система. – Дата доступа: 27.03.2025.

5. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 17 февр. 2025 г. № 61-З // ilex : информ : правовая система. – Дата доступа: 27.03.2025.

6. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. : в ред. Закона Респ. Беларусь от 17 февр. 2025 г. № 61-З // ilex : информ : правовая система. – Дата доступа: 27.03.2025.

7. Андрей Швед рассказал о принятых мерах предупреждения и пресечения киберпреступлений [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2025/february/87692/. – Дата доступа: 29.03.2025.

8. Комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2024 – 2025 годы [Электронный ресурс]. – Режим доступа: https://sh10.zhlobinedu.by/wp-content/uploads/2023/11/202-378-%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D1%8B%D0%B9-%D0%BF%D0%BB%D0%B0%D0%BD.pdf . – Дата доступа: 29.03.2025.