К ВОПРОСУ О БЕЗОПАСНОСТИ ГОСУДАРСТВА В ЭПОХУ ЦИФРОВИЗАЦИИ

Сушкова Юлия Сергеевна

студент, Донской государственный технический университет, РФ, г. Ростов-на-Дону

Осипова Юлия Валерьевна

научный руководитель, канд. филос. наук, доцент, Донской государственный технический университет, РФ, г. Ростов-на-Дону

Аннотация. В условиях стремительного развития цифровых технологий и их интеграции в различные сферы общественной жизни, обеспечение безопасности государства приобретает новые аспекты и вызовы. Цифровизация создает как возможности, так и угрозы, требующие комплексного подхода к формированию стратегий безопасности. В данной статье рассматриваются ключевые аспекты обеспечения государственной безопасности в эпоху цифровизации.

Ключевые слова: Цифровизация, государство, кибербезопасность, искусственный интеллект, правовое регулирование, государственное управление, новые технологии, интернет, киберугрозы, кибератаки.

Цифровизация является одним из наиболее значимых процессов современности, оказывающим глубокое влияние на все сферы жизни общества. Она открывает новые горизонты для экономического роста, улучшения качества жизни граждан и повышения эффективности государственного управления. Однако наряду с положительными аспектами цифровизация также порождает ряд угроз, способных подорвать основы государственной безопасности. В связи с этим возникает необходимость переосмысления традиционных подходов к обеспечению безопасности в условиях новых реалий.

Россия входит в число стран, наиболее подверженных риску кибератак. Это связано, прежде всего, со спецификой геополитического положения нашей страны и довольно низким уровнем инвестиций в защиту информационной инфраструктуры. Между тем, обеспечение безопасности обусловлено наличием внутренних проблем аппарата, а также знанием национальных и международных правовых норм в области оцифровки данных. Разработка стратегии кибербезопасности с юридической точки зрения делает государство лучше подготовленным к борьбе с киберрисками.

Вместе с тем, в современных условиях особенно актуальным становится вопрос адаптации кадрового потенциала к быстро меняющимся требованиям цифрового пространства. Многие государственные служащие и специалисты, ответственные за обеспечение безопасности, нуждаются в постоянном повышении квалификации и освоении новых компетенций. От этого напрямую зависит способность государственных структур адекватно реагировать на возникающие киберугрозы и своевременно адаптировать стратегию защиты информационных ресурсов.

Вместе с повышением квалификации персонала следует обращать особое внимание на формирование комплексной системы защиты критически важных объектов инфраструктуры.

Речь идёт не только о государственных учреждениях, но и о стратегических отраслях, таких как энергетика, транспорт, связь, банковский сектор. Сбои или атаки в этих сегментах могут иметь колоссальные последствия для всей страны, вплоть до остановки экономической деятельности или нарушения общественного порядка. Поэтому усиление безопасности ключевых объектов становится приоритетной задачей, требующей тесного взаимодействия государственных органов, бизнеса и научного сообщества.

Неотъемлемой частью современной системы государственной безопасности становится разработка чётких правовых механизмов, регулирующих использование инновационных технологий, включая блокчейн, большие данные (Big Data) и системы искусственного интеллекта. Такое регулирование необходимо, чтобы своевременно выявлять потенциальные риски и обеспечивать защиту конфиденциальной информации. В мировой практике наблюдается тенденция к созданию единых стандартов безопасности, которые устанавливают унифицированные требования к разработке и эксплуатации цифровых продуктов, что облегчает международное сотрудничество и обмен передовым опытом.

Ещё одним аспектом, заслуживающим пристального внимания, является формирование этических норм в сфере цифровизации. Вопросы этики приобретают особую значимость в ситуациях, когда использование передовых технологий способно затрагивать права и свободы граждан. Например, автоматизированные системы видеонаблюдения с элементами распознавания лиц и поведенческих паттернов могут повысить уровень общественной безопасности, но при этом создают риски избыточного вмешательства в частную жизнь. Сбалансированное правовое и этическое регулирование даёт возможность развивать потенциал цифровых технологий, не нанося ущерба правам граждан и демократическим институтам.

Таким образом, безопасность государства в эпоху цифровизации охватывает широкий спектр вопросов, начиная от технологических разработок и создания резервных систем защиты до совершенствования законодательства и формирования новой культуры кибергигиены. Именно комплексный подход, сочетающий технические, правовые и организационные меры, позволит укрепить устойчивость государственных структур и сохранить суверенитет в условиях стремительно меняющейся технологической среды.

Список литературы:

1. Корнев Л.В. Обеспечение информационной безопасности в условиях цифровизации / Л.В. Корнев // Молодой ученый. – 2022. – № 12

2. Хочуева Ф.А., Шугунов Т.Л., Жуков А.З., Ингушев Ч.Х. Информационная безопасность сквозь призму цифровой экономики // Современные наукоемкие технологии. – 2018. – № 11

3. Сухаренко А. Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. – 2018. – № 2