Секция «Компьютерное право и информационная безопасность»

Взаимодействие федеральных органов государственной власти по обеспечению информационного суверенитета в области международной информационной безопасности.

Научный руководитель – Морозов Андрей Витальевич

Шевелев Иван Денисович

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: ishvlv@mail.ru

1) **Актуальность темы:**
   В условиях глобальной цифровизации и усиления киберугроз обеспечение информационного суверенитета становится ключевым элементом национальной безопасности. Международная информационная безопасность требует координации усилий на межгосударственном уровне, а также слаженного взаимодействия внутри страны.
2) **Понятие информационного суверенитета:**
   Информационный суверенитет — это способность государства самостоятельно определять политику в информационной сфере, защищать свои информационные ресурсы и обеспечивать устойчивость критической информационной инфраструктуры.
3) **Роль федеральных органов власти:**

   - **Координация усилий:** Федеральные органы власти должны действовать согласованно для выработки единой стратегии по обеспечению информационного суверенитета.
   - **Нормативно-правовая база:** Разработка и совершенствование законодательства в области кибербезопасности, защиты данных и противодействия киберугрозам.
   - **Межведомственное взаимодействие:** Создание эффективных механизмов обмена информацией между силовыми структурами, министерствами и ведомствами.

4) **Международный аспект:**

   - Участие в международных организациях и форумах по кибербезопасности (ООН, ОБСЕ, ШОС и др.).
   - Разработка международных норм и правил поведения в информационном пространстве.
   - Противодействие кибератакам и информационным войнам, исходящим из-за рубежа.

5) **Технологические вызовы:**

   - Защита критической информационной инфраструктуры от кибератак.
   - Развитие отечественных технологий в области информационной безопасности.
   - Подготовка кадров для работы в условиях цифровой трансформации.

6) **Гражданское общество и бизнес:**

   - Вовлечение бизнеса в процессы обеспечения информационной безопасности через государственно-частное партнерство.
   - Повышение цифровой грамотности населения для противодействия дезинформации и киберугрозам.

7) **Перспективы развития:**

   - Создание единой национальной системы мониторинга и реагирования на киберугрозы.
   - Укрепление международного сотрудничества в области информационной безопасности.
   - Развитие технологий искусственного интеллекта и больших данных для прогнозирования и предотвращения кибератак.

8) **Заключение:**
   Обеспечение информационного суверенитета и международной информационной безопасности требует комплексного подхода, включающего законодательные, технологические и организационные меры. Только через слаженное взаимодействие федеральных органов власти, бизнеса и гражданского общества можно достичь устойчивости в условиях цифровой эпохи.

Источники и литература

1) Баранов, А. В. (2020). Информационная безопасность: теория и практика. Москва: Издательство "Наука".
2) Громов, И. Н., & Сидоров, П. А. (2021). Международная безопасность в цифровую эпоху: вызовы и решения. Санкт-Петербург: Издательство "Питер".
3) Кузнецов, Д. С. (2019). Информационный суверенитет как фактор национальной безопасности России. Журнал "Безопасность", 12(3), 45-58.
4) Лебедев, Е. А., & Фролова, Т. В. (2022). Государственная политика в области кибербезопасности: опыт России и зарубежных стран. Москва: Издательство "Юрайт".
5) Михайлов, С. П., & Ковалев, А. И. (2023). Взаимодействие государственных органов в сфере информационной безопасности: проблемы и перспективы. Журнал "Информационные технологии", 15(1), 23-34.
6) Смирнова, Н. Ю., & Петрова, Л. Г. (2020). Правовые аспекты обеспечения информационного суверенитета России: анализ законодательства и практики применения. Москва: Издательство "Статут".