

от 26.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

2. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс]: 6 января 2021 г., №91-3: принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ [Электронный ресурс] // СПС «Гарант». – 2021.

4. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 [Elektronische ressource]. – Zugriffsmodus: https://www.legislation-line.org/download/id/8253/file/Germany_CC%20am2019_de.pdf. Access-datum: 02.11.2021.

5. Code pénal du 1er novembre 2018 [Ressource électronique]. – Mode d'accès: https://www.legislationline.org/download/id/8273/file/Luxembourg_Criminal_Code_am2018_fr.pdf. Date d'accès: 02.11.2021.

ПОНЯТИЕ И ВИДЫ ИНФОРМАЦИОННОГО ОРУЖИЯ

Т.В. Сафонова, А.В. Будько

Ключевые слова: информационное оружие, информационная война, информационное противоборство, международное информационное право.

Информационное оружие представляет собой технические, программные и психологические приемы и способы информационного воздействия на противника, применяемые в условиях информационного противоборства (информационной войны).

Информационная война – война нового типа, объектом которой являются объекты информатизации, включая интернет-ресурсы, информационные системы, сети и сознание людей [1, с.134].

В соответствии с Соглашением, заключенным между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 года, информационная война представляет собой противоборство между двумя или более государствами в информационном пространстве в целях нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массовой психологической обработки населения для дестабилизации общества и государства, а

также принуждения государства к принятию решений в интересах противоборствующей стороны [2]

В этом же международном соглашении содержится понятие информационного оружия, под которым понимаются информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

Полагаем, целесообразно выделять информационно-техническое, информационно-программное и информационно-психологическое оружие.

К информационно-техническому оружию относятся средства радиоэлектронной борьбы, источники мощного электро-магнитного излучения, средства силового радиоэлектронного подавления, сверхмощные генераторы СВЧ-излучения и др.

К информационно-программному оружию можно отнести программные средства вывода из строя оборудования, преодоления систем защиты; сбора данных, циркулирующих в информационных системах противника; несанкционированного доступа; модификации компьютерной информации и программного обеспечения; уничтожения, блокирования, приведения в непригодное состояние компьютерной информации или программы, либо средства вывода из строя компьютерного оборудования, разрушения компьютерной системы, сети или машинного носителя и иные программные средства, эффективно решающие задачи информационной войны.

К информационно-психологическому оружию относят средства воздействия на сознание и подсознание людей: дезинформация посредством СМИ, социальных сетей, интернет-ресурсов, использование наркотических веществ, галлюциногенов, антидепрессантов и иных специально структурированных препаратов, средств виртуальной реальности, психотехник, нейролингвистического программирования, использование скрытых вставок, воздействующих на сознание и подсознание людей и многое другое [1].

В процессе применения информационного оружия становится не важным, как человек при этом относится к тому, что он видит и слышит; важно, чтобы он был постоянным пользователем, включенным потребителем информации, поскольку в этом случае на него можно целенаправленно и устойчиво воздействовать ежедневно и ежечасно.

Отличия информационного оружия от традиционных видов оружия заключаются в следующем:

- универсальность (применяется независимо от места, времени);
- латентность (позволяет вести наступательные действия скрытно, анонимно, без объявления войны);
- многочисленность форм реализации (легко маскируется под различные виды законной деятельности: обучающие и развивающие программы, семинары и тренинги и др.; аудиовизуальную продукцию: компьютерные игры, видеофильмы, мультфильмы, музыкальные композиции, печатные издания, реклама и др.);

- радикальность воздействия (коренным образом воздействует на информационные и компьютерные системы и сети, сознание и подсознание личности; ведет к коренным преобразованиям в обществе и государстве);
- экономичность (небольшие ресурсные вложения – чрезвычайно опасные последствия).

Следует отметить, что темпы совершенствования информационного оружия превышают темпы развития технологий и средств защиты. В связи с этим, задача нейтрализации угроз применения информационного оружия минимизации последствий его применения, должна рассматриваться как одна из приоритетных задач в сфере обеспечения информационной безопасности Республики Беларусь и приоритетное направление в обеспечении национальной безопасности Республики Беларусь в целом.

Информационное оружие сопоставимо с оружием массового поражения, которое направленно не столько на объекты информатизации, сколько на сознание людей, поражает его, разрушает способы и формы идентификации личности, создает личность с заранее заданными параметрами.

Республика Беларусь принимает необходимые меры для защиты своих граждан от деструктивного информационного воздействия, своей культуры, истории, традиций и духовных ценностей от уничтожения.

В настоящее время не существует международно-правовых и конституционно-правовых основ, запрещающих разработку и использование информационного оружия, однако Республика Беларусь и Российская Федерация, должны выступить инициаторами заключения разумных соглашений, опирающихся на принципы международного права.

Понятие информационной войны и информационного оружия должны найти законодательное закрепление на уровне национального законодательства.

Список использованных источников:

1. Информационное право: интерактивный курс лекций / Т.В. Сафонова. – 2-е изд. – Витебск: Издательство ВГУ им. П.М.Машерова, 2021. – 152 с.
2. Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // ЭТАЛОН. Международные договоры / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.