ВВЕДЕНИЕ

Современные информационные технологии не только открывают безграничные возможности для развития российского общества, но и порождают новые проблемы, вызовы и угрозы его безопасности, одна из важнейших ее составляющих — информационная безопасность. Однако информационно-коммуникационные технологии (далее — ИКТ), как и любые другие, сами по себе не являются ни плохими, ни хорошими — их свойства одновременно могут представлять собой и угрозу, и благо. Все зависит от целей их использования, которые определяются обществом и могут быть применены не только для обеспечения благополучия человечества, но и для организации тотального контроля, ведения информационных войн и т.д. По некоторым данным, свыше 120 стран разрабатывают концепции информационных войн с использованием принципиально нового оружия — информационного[1], тогда как разработки в области ядерного оружия ведутся не более чем в 20 странах[2].

Информационная безопасность, являясь стратегическим национальным приоритетом Российской Федерации, зависит от уровня ее обеспечения, и в ходе технического прогресса с расширением применения ИКТ эта зависимость возрастает. Значимость информационной безопасности для Российской Федерации обусловлена в том числе тем, что информационная сфера обеспечивает функционирование всех остальных сфер жизни общества и государства.

Ранее национальная безопасность рассматривалась как сохранение суверенитета и территориальной целостности государства, его устойчивость перед угрозой применения вооруженной силы со стороны

---

1 См., например: Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М., 2005.

2 Там же. С. 235.

других государств. В настоящее время она видится как комплексная системная проблема, учитывающая наличие многообразных факторов и угроз, в первую очередь информационных.

Информационное оружие подрывает традиционное понятие государственных границ, используется достаточно скрытно, не нуждается в тщательной подготовке. Жертва атаки может даже и не подозревать о том, что находится под информационным ударом, в силу чего значительно ограничивается возможность противодействовать такой агрессии. Это не является проблемой, специфичной только для Российской Федерации — практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности.

Время, новые технологии, вызовы и угрозы меняют приоритеты, требования к информационной безопасности, что предполагает адекватное реагирование на них. На характер и направленность угроз влияет и политическая ситуация в мире. С начала специальной военной операции России на Украине число кибератак увеличилось в разы. Вице-премьер Российской Федерации Д. Чернышенко привел такие цифры: в 2022 г. было отражено около 50 тыс. хакерских атак на российские информационные ресурсы. При этом если в 2021 г. атаки были направлены главным образом на финансовый сектор, то в 2022 г. акцент сместился на государственный. Имеются данные и в отношении кибератак в первой половине 2023 г. — их число увеличилось на 65%[3]. По мнению заместителя директора Национального координационного центра по компьютерным инцидентам Н. Мурашова, цель такой киберкомпании — вывести из строя информационную инфраструктуру России и получить доступ к системам организаций и предприятий[4]. Так, в 2023 г. кибератаке подверглись информационные

[3] URL: http://www.vedomosti.ru
[4] Там же.

системы МЧС России, таможенных органов. В настоящее время резко выросло число кибератак на российские IT-компании.

Кибератаки — одна из основных, но не единственная угроза информационной безопасности. На уровне отраслевого законодательства конкретизируются соответствующие положения с учетом существующих особенностей (информационная безопасность критической информационной инфраструктуры, медицины, образования, персональных данных и др.).

Информационная война все больше активизируется посредством деструктивного информационно-психологического воздействия на население, дезинформации и фейков, манипуляции массовым сознанием, утечки информации. Все эти угрозы требуют скорейшей и адекватной реакции, восстановления и поддержания национальной информационной безопасности на должном уровне.

Активное развитие и внедрение во все сферы жизни новых информационно-телекоммуникационных технологий сопровождаются появлением все новых угроз безопасности граждан, общества и государства, активизацией уже существующих угроз. Влияние новых технологий на информационную безопасность, характер рисков показаны в гл. 2 настоящей работы, где рассматривается воздействие на информационную безопасность технологий искусственного интеллекта (далее — ИИ), машиночитаемого права, «больших данных», технического регулирования и стандартизации, технологий распределенного реестра и систем ИИ.

Особое внимание в монографии уделено информационной безопасности личности. Рассматриваются состояние информационной защищенности человека и направления ее обеспечения в различных сферах, в том числе в таких значимых и чувствительных, как медицина, обращение лекарственных средств, образование, защита персональных данных, коррупция и т.д. Определяются пути преодоления существующих проблем, среди которых одна из основных — защита персональных данных. В аналитическом отчете «Россия: утечки

информации ограниченного доступа в 2022 году», подготовленном экспертно-аналитическим центром InfoWatch, приводятся следующие данные: за год (2022 г.) утечка записей персональных данных и платежной информации увеличилась в 2,67 раза по сравнению с 2021 г., что в 4,5 раза превысило население России[5].

Нарушение информационной безопасности может быть связано не только с умышленным совершением правонарушений, преступных деяний в информационной сфере, но и с организацией электронного взаимодействия, передачей, хранением электронных документов, что предполагает формирование единой цифровой среды доверия для снижения угрозы информационной безопасности, причинения вреда и для обеспечения надежного документооборота.

В работе отражен и зарубежный опыт противодействия информационным опасностям. Показательно, что меры, принимаемые государством (объединением государств), могут носить политический, технологический, юридический, управленческий или военный характер, а также соответствуют конкретным рискам[6]. Следует отметить, что предпринимаемые другими государствами меры сходны с российскими.

Юридическая наука на современном этапе сталкивается с необходимостью решения новых задач, пересмотра традиционных правовых подходов, в том числе относительно информационной безопасности в условиях цифровизации. Авторский коллектив выражает надежду, что монография будет представлять интерес как для ученых-юристов, так и для широкого круга читателей.

---

5 См.: Utechki_informatsii_ogranichennogo dostupa. URL: http://www.infowatch.ru

6 См.: Strategii kiberbezopasnosti-gosudarstv ES. URL: http://www.infowatch.ru