Секция «Компьютерное право и информационная безопасность»

Правовой анализ информационной безопасности в сфере отечественной промышленности

Научный руководитель – Зуева Анна Сергеевна

Кулик Павел Александрович
Выпускник (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия
E-mail: pasha73900@gmail.com

В условиях стремительного развития цифровых технологий и их интеграции в промышленный сектор России, обеспечение информационной безопасности отечественной промышленности приобретает первостепенное значение. Угроза кибератак, промышленного шпионажа и несанкционированного доступа к конфиденциальной информации требует правового анализа и разработки эффективных механизмов защиты.

В первую очередь необходимо раскрыть рассматриваемого нами понятия. Под информационной безопасностью в промышленности необходимо понимать состояние защищенности информационных ресурсов и систем управления технологическими процессами от внутренних и внешних угроз, что включает в себя защиту от несанкционированного доступа, утечки данных, кибератак и иных форм информационного воздействия, способных нанести ущерб как отдельным предприятиями, так и промышленным конгломератам, что в свою очередь может привести к возникновению экономических потерь для государства. Отдельное внимание необходимо уделить критической информационной инфраструктуре, сбои в работе которой могут привести к серьезным последствиями для национальной безопасности.[n1]

Современные промышленные предприятия все больше зависят от автоматизированных систем управления технологическими процессами (далее – АСУ ТП), которые интегрированы в единую информационную среду. Любое вмешательство в их работу может привести к сбоям в производственных процессах, что может привести к значительным космическим потерям и даже катастрофам техногенного характера. На основании чего мы можем сказать, что на первый план выходит разработка эффективных правовых механизмов регулирования АСУ ТП.[n2]

Одним из ключевых актов, регулирующих рассматриваемую сферу, является Постановление Правительства РФ № 127. Данный акт раскрывает вопрос категоризации объектов критической информационной инфраструктуры (далее – КИИ).[n3] Не менее важным регулятором является Приказ ФСТЭК России № 235, в котором раскрываются требования к разрабатываемым КИИ.[n4]

Однако несмотря на существенную нормативную правовую базу в рассматриваемой сфере существуют определенные проблемы. Одной из таковых является низкий уровень осведомленности и квалификации персонала промышленных предприятий в вопросах кибербезопасности. Отсутствие квалифицированных специалистов, а также недостаток внимания к обучению сотрудников, что влечет к образованиям уязвимостей в системах, которыми в последующем пользуются злоумышленники.

В качестве иной проблемы также можно выделить необходимость постоянного обновления и совершенствования технических средств защиты информации. Быстрое развитие технологий приводит к появлению новых видов угроз, что требует адекватного и своевременного реагирования со стороны предприятий и государства.

Существует необходимость в усилении международного сотрудничества в области кибербезопасности, поскольку многие угрозы имеют трансграничный характер, также существует ряд международных, совместных с Россией производственных предприятий. Обеспечение обмена информацией и своевременная разработка стандартов безопасности могут повысить эффективность защиты отечественной промышленности от киберугроз. [n5]

На основании ранее изложенного, на наш взгляд для устранения существующих проблем необходимо совершить следующий ряд действий правового характера: разработать новые меры по стимулированию предприятий к внедрению современных технологий защиты информации; усилить контроль за выполнением требований законодательства в сфере информационной безопасности; обеспечить интеграцию отечественных стандартов информационной безопасности с международными нормами и практиками.

Таким образом, обеспечение информационной безопасности в сфере отечественной промышленности является комплексной задачей. Совершенствование нормативной правовой базы, повышение квалификации специалистов, внедрение современных технологий защиты – ключевые направления, способные обеспечить надежную защиту информационных ресурсов российских предприятий.

Источники и литература

1) Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ // [Электронный ресурс]: https://www.consultant.ru/document/cons_doc_LAW_220885/
2) Шибаев, Д. В. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Д. В. Шибаев ; Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА). – Вологда : Северо-Западный ин-т(филиал) Ун-та им. О. Е. Кутафина (МГЮА), 2024. С. 81.
3) Постановление Правительства РФ от 08.02.2018 N "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" // [Электронный ресурс]: https://www.consultant.ru/document/cons_doc_LAW_290595/
4) Приказ ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" // [Электронный ресурс]: https://www.consultant.ru/document/cons_doc_LAW_291501/
5) Антонян Е.А. Международное сотрудничество в сфере противодействия кибертерроризма // научная статья. Ж.: «Правовой альманах». 2022г. С. 13