УДК 349.6: 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИЧЕСКОМ ПРАВЕ: НАЦИОНАЛЬНЫЙ И МЕЖДУНАРОДНЫЙ АСПЕКТЫ

А. С. Греков
Белорусский государственный экономический университет

Аннотация

В статье рассматриваются вопросы информационной безопасности (ИБ) применительно к экологическому праву. Исследуется значение ИБ для национальной и международной безопасности, раскрывается роль ИБ в экологическом праве. По итогам исследования раскрыто значение ИБ в экологическом праве в аспекте охраны окружающей среды и определены основные направления развития в данном вопросе на национальном и международном уровне. Автор аргументирует положения о том, что ИБ, применительно к охране окружающей среды, – фактор, обеспечивающий благоприятное существование человека и функционирование государства.

Ключевые слова: охрана окружающей среды, информационная безопасность, киберпространство, киберпреступления, искусственный интеллект.

Экологическое право – комплексная отрасль права, нормы которой регулируют отношения, складывающиеся в процессе охраны окружающей среды. Благоприятная окружающая среда – один из ключевых факторов существования человека. Любые изменения состояния окружающей среды могут негативно воздействовать как на население одной страны, так на человечество в целом. Информационная безопасность является одним из основных элементов, способствующих поддержанию окружающей среды на достаточном для существования человека уровне в рамках государственного и международного правового регулирования.

Актуальность данной работы заключается в раскрытии значения информационной безопасности в экологическом праве в аспекте охраны окружающей среды и определении основных направлений развития в данном вопросе на национальном и международном уровне.

Информационная безопасность является одним из элементов, составляющих общую национальную безопасность в Республике Беларусь, а также международную безопасность в отношении всего мирового сообщества. Концепция национальной безопасности Республики Беларусь, утвержденная Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 (далее – Концепция национальной безопасности), определяет основные направления обеспечения безопасности и закрепляет такое понятие, как информационная безопасность. Согласно ст. 4 Концепции национальной безопасности, под информационной безопасностью следует понимать: «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и

внутренних угроз в информационной сфере». При этом можно отметить, что непосредственное обеспечение информационной безопасности связанно с национальными интересами в данной сфере. К ним можно отнести: формирование и поступательное развитие информационного общества; равноправное участие Республики Беларусь в мировых информационных отношениях; преобразование информационной индустрии в экспортно-ориентированный сектор экономики; эффективное информационное обеспечение государственной политики; обеспечение надежности и устойчивости функционирования критически важных объектов информатизации и др. Перечисленные интересы напрямую или косвенно могут влиять на состояние окружающей среды.

Понятие и сущность информационной безопасности неразрывно связаны с понятием киберпространства. В законодательстве Республики Беларусь легально закреплено определение понятия «киберпространство». Оно содержится в Концепции обеспечения кибербезопасности в банковской сфере, утвержденной Постановлением правления Национального банка Республики Беларусь от 20 ноября 2019 г. № 466 (далее – Концепция обеспечения кибербезопасности), где под киберпространством понимается «... виртуальное пространство (среда), предоставляющее возможности для осуществления коммуникаций и (или) реализации общественных отношений, образовавшихся в результате функционирования технологий, устройств и сетей, объединенных в коммуникационные системы, и обеспечивающее электронные коммуникации с использованием сети Интернет и (или) других сетей передачи данных».

Международное право, в отличие от законодательства Республики Беларусь, не устанавливает легальную дефиницию киберпространства. Ближе всего к разработке понятие подошло Таллиннское руководство (далее – Руководство) созданное в 2017 году группой экспертов в сфере международного права ведения войны. Руководство рассматривает вопросы ведения военных действий в киберпространстве, учитывая принципы и нормы современного гуманитарного права. Исходя из доктринального толкования, основываясь на положениях Руководства, которое на сегодняшний день представляет собой наилучшую попытку адаптировать традиционное международное гуманитарное право к киберпространству, можно отметить, что под киберпространством понимается коммуникативный, хранилищный и вычислительный ресурс, на котором работает информационная система. Экологические идеи, нормы и дискуссии, а также эпистемологические сообщества, которые их порождают, меняются и адаптируются к меняющемуся контексту, в котором уславливается международное экологическое права [1, с. 253]. Такие изменения касаются также информационной безопасности.

Любые формы взаимодействия в киберпространстве могут влиять на информационную безопасность. Посредством киберпространства возможно нарушение порядка функционирования инфраструктуры и деятельности государства. Такие деяния можно отнести к киберпреступлениям.

Вследствие киберпреступления может быть нанесен не только материальный, но и экологический ущерб. Негативное воздействие на

информационно-техническое обеспечение инфраструктур, необходимых для существования человека, представляет значительный уровень угрозы не только для государства, но и международного сообщества в целом. К подобного рода критически важным инфраструктурам можно отнести: станции по очистке воды для питьевого потребления населением, станции по переработке вредных веществ, атомные электростанции, станции энергоснабжения населения и др.

Таким образом, информационная безопасность, наравне с иными видами безопасности, имеет большое значение для охраны окружающей среды и как следствие, для экологического права Республики Беларусь и для права окружающей среды на международном уровне.

Учитывая современные тенденции развития технологий и информатизации, стоит говорить о возникновении новых элементов регулирования в сфере информационной безопасности применительно к охране окружающей среды. К таким элементам могут быть отнесены: искусственный интеллект (далее – ИИ), вопрос защиты экологически значимой информации, вопрос обеспечения информационной безопасности экологически значимых объектов инфраструктуры.

ИИ можно в основном определить как мимикрию человеческого интеллекта посредством применения информационных технологий или машин. Когнитивные функции человеческого сознания, такие как обучение, решение проблем, вариативность мышления, копируются машиной. Текущие разработки в области вычислительной техники могут быстро и точно собирать информацию в большом объеме, что превосходит человеческие возможности. Автономные системы могут быть запрограммированы на учёт большого количества переменных и применять более строгие процедуры [2, с. 118]. Поэтому можно также определить ИИ как машину, которая способна применять алгоритмы человеческого мышления и решать проблемы, основываясь на выборе, самостоятельно.

В целом ИИ позволит людям качественнее выполнять свою работу и повысит эффективность, одновременно сократив расходы за счет устранения ненужных процессов. ИИ возьмет на себя аналитические задачи, такие как обработка данных, формирование оперативных баз данных, проектирование и прогнозирование в сфере охраны окружающей среды. ИИ позволит выполнять поставленные задачи быстрее и более полноценно и сократить время, необходимое на его выполнение. Наравне с этим ИИ способствует обеспечению информационной безопасности путем контроля киберпространства в сфере его применения.

Применительно к экологическому праву ИИ может применяться в различных областях. Например, при загрязнении окружающей атмосферы. Загрязнение атмосферы является широко распространенной проблемой во всем мире. Это то, что непосредственно вредит здоровью человека. В Китае, где расположены одни из самых загрязненных городов мира, IBM запустила свой проект Green Horizon, в котором используется технология ИИ для отслеживания и прогнозирования уровней загрязнения воздуха, поиска источников такого загрязнения и предоставления потенциальных решений для

борьбы с загрязнением воздуха. Учитывая, что все программное управление находится в рамках ИИ, особую опасность представляют киберпреступления, направленные на нарушение деятельности подобного рода программы. В случае отключения системы по контролю уровня загрязнения посредством кибератаки население и окружающая среда будут подвержены загрязнению, и, в конечном итоге, к экологической катастрофе.

Следующий элемент – вопрос защиты экологически значимой информации. Информация играет ключевую роль для разрешения вопросов, связанных с охраной окружающей среды. От объема и качества получаемой и содержащейся информации зависит правильность решений в области реагирования на изменения состояния окружающей среды.

К экологически значимой информации в данной сфере можно отнести: информацию о размещении экологически опасных производств; информацию о потенциальных экологических угрозах здоровью и жизни человека; информацию об уровне загрязнения воздуха, земли, вод, недр; информацию о местах переработки и свалки вредных отходов; информацию о функционировании атомных электростанций; информацию о размещении и хранении ядерных материалов; информацию о размещении и хранении ядерного и иного вооружения и др. информацию, посредством которой возможно воздействовать на состояние окружающей среды.

Вопрос защиты данных в киберпространстве напрямую связан с охраной окружающей среды. Киберпреступники посредством завладения экологически значимой информацией могут организовывать преступления, которые подвергают опасности не только благоприятное состояние окружающей среды, но, как следствие, жизнь и здоровье населения конкретного государства и человечества в целом. В качестве примера можно привести такое преступление, как террористический акт на объекты инфраструктуры, необходимые для обеспечения должного уровня состояния окружающей среды, или повреждение которых может неблагоприятно воздействовать на состояние окружающей среды.

Оставшийся элемент – вопрос обеспечения информационной безопасности экологически значимых объектов инфраструктуры. Учитывая развитие современных технологий, можно прогнозировать, что в ближайшем будущем большинство объектов инфраструктуры будут переведены на собственное программное управление, в т. ч. благодаря ИИ. В связи с этим защита подобного рода инфраструктур, к которым можно отнести станции по очитке воды для питьевого потребления населением, станции по подаче или распределению электроэнергии, объекты, связанные с производством пищевой продукции и др., имеет особо важное значение для государства и международного сообщества в целом.

Нарушение деятельности данных объектов может стать целью киберпреступников для дестабилизации общества и нарушения экономического строя государства и благоприятного состояния окружающей среды в мировом масштабе. Учитывая тот факт, что экологический ущерб не ограничивается территорией одного государства, защита и обеспечение информационной

безопасности такого рода объектов должно стать задачей не только одного государства, в котором происходит катастрофа, но и всего мирового сообщества в целом.

Исходя из вышеизложенных фактов можно сделать следующий вывод. Информационная безопасность – необходимый элемент, способствующий обеспечению национальной и международной безопасности. Поддержание благоприятного состояния окружающей среды, а также её охрана остаётся одной из основных задач не только государства, но и мирового сообщества в целом. Информационная безопасность в экологическом праве в аспекте охраны окружающей среды представляет собой комплекс мер по правовому регулированию безопасности и сохранности окружающей среды от воздействия посредством киберпространства.

Развитие информационно-коммуникационных технологий активизирует сотрудничество государств по правовому регулированию вопросов безопасности в киберпространстве относительно охраны окружающей среды. Развитие программного управления и ИИ ставят новые вызовы перед международным сообществом и законодателем Республики Беларусь в отношении правового регулирования вопросов информационной безопасности. Защита объектов, обеспечивающих жизнь и здоровье человечества, учитывая потенциальное воздействие через киберпространство, представляет собой важный аспект национальной и международной безопасности. Вопросы кибербезопасности, поскольку посредством нее возможно воздействие на состояние окружающей среды, должны быть урегулированы как на международном, так на национальном уровнях, с учетом развития научно-технического прогресса.

Список использованных источников:

1. Lavanya, R. The Oxford handbook of International environmental law : Second Edition / R. Lavanya, Jacqueline P. – New York ; Oxford : Oxford Univ. Press, 2021. – 1225 p.

2. Греков, А. С. Угроза экологической безопасности государств при ведении военных действий с использованием автономных систем / А. С. Греков // Киберугрозы как новый вызов для международного гуманитарного права : сборник материалов студенческой научно-практической конференции, Минск, 27 мая 2022 г. / УО «Международный университет «МИТСО»; редкол.: О. М. Старовойтов [и др.] ; под общ. ред. О. М. Ленцевич. – Минск: МИТСО, 2022. – С. 116–119.