УДК 343.34

Кузьминова А.А.
студент
СГТУ им. Гагарина Ю.А.
Российская Федерация, Саратов
Ризина М.А.
Студент
СГТУ им. Гагарина Ю.А.
Российская Федерация, Саратов
Научный руководитель: Фролов В.В., д.б.н.
профессор кафедры «Государственное правовое регулирование экономики и кадровой политики»
СГТУ им. Гагарина Ю.А.
Российская Федерация, Саратов

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация: В данной статье рассматривается вступление мирового сообщества в эпоху информационных технологий, которые используются во всех сферах жизни человека. При этом необходимо подчеркнуть, что развитие цифровых технологий привело к возникновению нового вида преступности – киберпреступности. В ходе исследования было выявлено, что киберпреступность является угрозой для экологической безопасности страны. Именно поэтому необходимо защищать общество и государство от виртуальной опасности. Для борьбы с киберпреступностью и для эффективного обеспечения экологической безопасности страны необходимо использовать системный подход, тщательно разрабатывать законодательную базу, а также интенсивно вести сотрудничество с другими странами.

Ключевые слова: информационные технологии, киберпреступность, экологическая безопасность, цифровые технологии, уголовная ответственность, окружающая среда.

A.A. Kuzminova
student
SSTU them. Gagarina Yu.A.
Russian Federation, Saratov
Rizina M.A.
Student
SSTU them. Gagarina Yu.A.
Russian Federation, Saratov
Scientific adviser: Frolov V.V., Doctor of Biological Sciences
professor of the department "State legal regulation of the economy and personnel policy"
SSTU them. Gagarina Yu.A.
Russian Federation, Saratov

CYBER CRIME AS A THREAT TO ENVIRONMENTAL SECURITY

Resume: This article examines the entry of the world community into the era of information technologies, which are used in all spheres of human life. It should be emphasized that the development of digital technologies has led to the emergence of a new type of crime - cybercrime. The study revealed that cybercrime is a threat to the country's environmental security. That is why it is necessary to protect society and the state from virtual danger. To combat cybercrime and effectively ensure the country's environmental security, it is necessary to use a systematic approach, carefully develop a legislative framework, and intensively cooperate with other countries.

Key words: information technology, cybercrime, environmental safety, digital technologies, criminal liability, environment.

В современном мире большое распространение получили информационные системы. Они вошли во все сферы жизни человека. Не является исключением и правовая сфера. Цифровые технологии в своем развитии открывают большое количество возможностей. Технологический прогресс идет быстрыми темпами во всех отраслях науки и промышленности. По мнению исследователей, внедрение новых технологий с каждым годом будет происходить все быстрее.

Цифровые технологии представляют собой уникальное явление, которое полностью изменило жизнь каждого человека. Сейчас все люди используют достижения прогресса для наиболее быстрой и простой передачи данных. Главными преимуществами цифровых технологий, благодаря которым они обрели свою популярность, стали универсальность и быстродействие.

Интернет позволяет создать копию настоящего физического мира. То есть каждый объект, который подключен к Интернету, может находиться под полным контролем владельца. Именно стремление к комфорту и повышению качества жизни населения приводит к созданию экологически чистых технологий, например, «умных» городов. Главным принципом их создания является использование информационных технологий, которые позволяют в режиме реального времени вычислять и корректировать направления развития города, принимая при этом экологические и рациональные решения.

В настоящее время разработано большое количество проектов «умных» городов. Увеличение их числа можно объяснить тем, что в результате интенсивного экономического роста увеличивается степень загрязнения окружающей среды. Основными источниками загрязнения

принято считать объекты промышленности, энергетики, транспорта и строительства. Это обуславливает необходимость использования экологичных и рациональных технологий, которые позволят стабилизировать и улучшить экологическую обстановку.

Но несмотря на большое количество преимуществ применения цифровых технологий, существуют и недостатки. Увеличение применения электронных технологий, количества пользователей сети Интернет происходит не только в экономике и политике, но и в преступной деятельности. С каждым днем появляется все больше видов общественно опасных деяний. Изменение самой преступности и облика преступника приводит к появлению нового явления – киберпреступности.

Киберпреступность представляет собой незаконное осуществление действий в электронной сфере, которое совершено с использованием компьютерных технологий или против них. К киберпреступности можно отнести любое преступление, которое совершено в электронной среде или с использованием цифровых технологий. Данный вид преступности обладает определенными особенностями, которые придают особую опасность данным деяниям:

- Максимальная скрытность деяний. Это достигается благодаря специальным методам анонимности, которые распространены в цифровой среде;
- Трансграничность. Данная характеристика предполагает разделение преступника и потерпевшего огромным расстоянием. Именно поэтому киберпреступность охватывает огромные территории, распространена во всех странах мира и является международной угрозой;
- Возможность совершения преступлений в автоматизированном режиме. Киберпреступники разрабатывают специальные программы, которые могут работать без их участия;

- Нестандартность действий преступников. Действия злоумышленников, практически, невозможно предусмотреть, а соответственно и предотвратить.

Таким образом, все вышеперечисленные особенности делают цифровые технологии очень привлекательными для совершения преступлений.

Так как количество преступлений в сфере компьютерных технологий возрастает с каждым днем, то можно говорить о возникновении новой угрозы для национальной безопасности страны. По Стратегии национальной безопасности России, которая принята Указом Президента РФ от 02.07.2021 года № 400, национальная безопасность представляет собой состояние защищенности личности, общества и государства от внутренних и внешних угроз, при которых обеспечиваются реализации конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие России. Частью национальной безопасности РФ является экологическая безопасность. Понятие термина «экологическая безопасность» обозначено в ФЗ «Об охране окружающей среды» от 10.01.2002 года. Экологическая безопасность – это состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий.

Киберпреступность несет угрозу национальной безопасности, а значит и экологической безопасности, как ее составляющей. Если учитывать все особенности киберпреступности, то можно сказать, что преступники не останавливаются на простых грабежах финансов. Они стали опасны в экологическом плане. Киберпреступники могут остановить

работу химических производств, комплексов энергоснабжения и водоснабжения, прекратить очистку сточных вод. Все эти преступления совершаются с использованием фальшивых виртуальных адресов, что затрудняет поиск виновных. Киберпреступники могут использовать специальные вредоносные коды, которые запускаются в систему и провоцируют аварию. В некоторых случаях может произойти экологическая катастрофа.

Из вышесказанного можно сделать вывод о том, что необходимо готовится к новым угрозам экологической безопасности. Эта необходимость обусловлена реализацией цифровых технологий в мировой экономике при наличии проблем с защитой от исходящей от них опасности в области обеспечения экологической безопасности. Обеспечение экологической безопасности в условиях цифровой экономики требует большое количество подготовительных мероприятий международного уровня.

Особое внимание специалисты по экологической безопасности уделяют ускоренному внедрению транспортной системы с искусственным интеллектом. Обеспечение экологической безопасности за счет искусственного интеллекта и учета внешних факторов может достигнуть 90%. Но наивысший уровень экологической безопасности может быть достигнут только при эффективном разделении работы роботов и человека.

Одной из важных функций государства является реакция на отклоняющееся поведение, но стоит отметить, что государство должно реагировать на особо опасные преступления. Для наиболее эффективной защиты общества от угроз в цифровой сфере необходимо решить несколько задач:

- Построение эффективной системы защиты информации и информационной системы;

- Систематизация уголовно-правового законодательства для эффективной борьбы с экономическими преступлениями.

В настоящее время происходит изменение правового законодательства. Помимо главы 28 УК РФ «Преступления в сфере компьютерной информации», в Уголовном кодексе наблюдается тенденция использования информационных технологий в квалифицирующих признаках преступлений. Данный квалифицирующий признак затрагивает практически все главы и разделы Уголовного кодекса. Также не исключением являются и преступления, которые являются угрозой экологической безопасности. Например, в ст.258 «Незаконная добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу РФ и (или) охраняемым международными договорами РФ» были внесены поправки в 2017 году. С того времени во второй части статьи содержится новый квалифицирующий признак, который устанавливает ответственность за совершение деяния в сфере информационных технологий.

Таким образом, законодательство реагирует на изменения, которые происходят в обществе, на новые угрозы, исходящие от цифровых технологий. Но стоит учитывать, что не всякое использование технологий можно назвать общественно опасным деянием. То есть квалифицирующий признак необходимо включать в состав преступления только в тех случаях, когда оно несет вредные последствия или убытки.

В заключение можно сказать, что несмотря на то, что обеспечение экономической безопасности меняется под влиянием использования цифровых технологий, не стоит масштабно и спонтанно менять законодательство, внося в него поправки об использовании технологий в преступлениях. Достаточно вносить изменения постепенно. Для эффективной борьбы с киберпреступлениями в области экологической

безопасности необходимо применять системный подход, разрабатывать нормативно-правовую базу и вести интенсивное международное сотрудничество.

Использованные источники:

1. Атаманов Г.А. Экологическая безопасность и ее место в структуре безопасности антропных систем // Наука XXI. – 2019. - № 3. – С. 52-59.
2. Глухова А.А. Новейшие способы совершения киберпреступлений как угроза экономической безопасности России // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. -№ 1. – С. 156-161.
3. Грешневиков А.Н. Проблемы экологической безопасности России // Право и безопасность. – 2020. -№ 2. – С. 15-30.
4. Кальнер В.Д. Цифровая экономика и экологическая безопасность жизнедеятельности // Экология и промышленность России. – 2018. – Т. 22, № 1. – С.62-67.
5. Королева А.Н. Правовое регулирование реализации экологических прав граждан на основе применения технологии «умный город» // Реализация и защита экологических прав граждан: сборник материалов всероссийской конференции по вопросам реализации и защиты экологических прав граждан. – 2018. –С.175-188.
6. Кудрявцев В.Н. Объективная сторона преступления / В.Н. Кудрявцев. – М.: Юрид. лит., 2015. – 218 с.