государства и бизнеса, эффективное управление проектом, удовлетворение потребностей общества в качественных товарах и услугах, координация со стороны государства, долгосрочная основа взаимоотношений путем заключения соглашения или иного правоустанавливающего документа дают основание рассматривать свободные зоны как особую форму ГЧП или как среду реализации ГЧП. Среду, имеющую локальный характер [3]. Однако при наличии схожих характеристик СЭЗ и ГЧП, необходимо не выпускать из вида принципиальное отличие – в рамках СЭЗ функционирует значительное количество резидентов, занимающихся различными видами деятельности.

Таким образом, применение методов и принципов государственно-частного партнерства (ГЧП) в экономике Республики Беларусь могло бы активизировать предпринимательскую и внешнеэкономическую деятельность и повысить инвестиционную привлекательность свободных экономических зон (СЭЗ).

Список использованных источников

1. Министерство экономики Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.economy.gov.by/ru/cez-lgoty-preferencii-ru/-Дата доступа: 03.11.2019.

2. Национальное агентство инвестиций и приватизации Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.investinbelarus.by/public-private-partnerships/-Дата доступа: 03.11.2019.

3. Думнов А.П. К вопросу регулирования государственно-частного партнерства в условиях особой экономической зоны // Вестник Бурятского государственного университета. Вып. 2. Экономика. Право. Улан-Удэ, Изд-во БГУ, 2010. С. 99–103.

УДК (004.514.6+004.056):343

Р.Н. Ключко
Гродненский государственный университет имени Янки Купалы

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ КАК ОБЪЕКТЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

В соответствии с Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 N 1, которая обеспечивает комплексный подход к проблеме информационной безопасности, под

информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере; в свою очередь кибербезопасность определяется как состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. Информационная инфраструктура понимается как совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации. Состояние защищенности последних гарантируется правовыми нормами, регулирующими различные виды комплексных информационных отношений, а также обеспечивающими их охрану от общественно опасных посягательств (глава 31 Уголовного кодекса Республики Беларусь; ст. 22.6 «Несанкционированный доступ к компьютерной информации», ст. 22.16. «Нарушение требований по использованию национального сегмента сети Интернет» КоАП Республики Беларусь), при этом кибербезопасность как объект правовой охраны в уголовном и административном законодательстве не упоминается.

Российские ученые Т.А Полякова, А.В. Минбалеев и И.С. Бойченко, указывают, что сформированная триада субъектов – личности, общества и государства, являющихся важнейшими субъектами отношений в области обеспечения информационной безопасности, в эпоху трансформации права испытывает на себе последствия процессов цифровизации. Следует согласиться с их утверждением о том, что процессы и проблемы цифровизации, требующие универсальных правовых средств, на основе междисциплинарных подходов организационно-правовых проблем в области информационной безопасности, при формировании единой цифровой среды доверия должны быть решены при помощи фундаментальной науки [1, с. 66].

Уголовное законодательство, обеспечивающее охрану информационной безопасности, должно содержать ясно определенные однозначные термины и понятия, соответствующие нормам регулятивных отраслей права. Однако следует констатировать, что в нем не только имеются пробелы в части правового обеспечения защиты информационной безопасности, но и используются категории и термины с недостаточной определенностью, не соответствующие понятийному аппарату норм других отраслей права, а в отдельных случаях и не в полной мере соответствующие духу уголовного закона, что затрудняет его применение и вызывает проблемы, связанные с правильной правовой оценкой совершенных общественно опасных деяний. Позволим себе остановиться лишь на проблеме анализа понятийного аппарата, используемого при определении родового понятия «преступления против информационной безопасности».

Стоит отметить, что в белорусской уголовно-правовой доктрине проблемы использования информации для совершения преступлений исследовались в контексте анализа преступлений против информационной безопасности без предложений именовать указанную группу преступлений информационными преступлениями [2 – 9]. Имелись предложения об объединении группы преступлений, совершаемых внутри и с использованием киберпространства, в одной главе «Киберпреступления» («Интернет-преступления») [10].

Нормы главы 31 Уголовного кодекса Республики Беларусь «Преступления против информационной безопасности» по сути обеспечивают уголовно-правовую охрану кибербезопасности. Информационная безопасность представляет собой более широкий объект уголовно-правовой охраны, так как сфера информационных отношений включает в себя как отношения, связанные с использованием информационно-коммуникационных технологий, в том числе и сети Интернет, так и отношения в сфере обращения различной информации (как составляющей, так и не составляющей предмет различных видов тайн), передаваемой любыми способами от одного субъекта другому.

Указанные обстоятельства обусловливают необходимость совершенствования понятийного уголовно-правового аппарата в соответствии с положениями всего массива нормативных правовых актов, имеющих регуляторное значение для развития информационных отношений. Заслуживающими внимания являются предложения российских исследователей об обеспечении гармонизации понятийного аппарата не только в рамках одного и/или группы нормативных правовых актов, актов рекомендательного характера, стандартов, а через всю иерархию информационного законодательства, а также в рамках как национального, так и наднационального права [1, с. 66, 67].

Список использованных источников

1. Полякова, Т.А. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права / Т.А. Полякова, А.В. Минбалеев, И.С. Бойченко // Вестник УрФО. – №3 (33). – 2019. – С. 64 – 68.

2. Ахраменка, Н.Ф. Преступления против информационной безопасности: краткий реестр проблем / Н.Ф.Ахраменка // Право и демократия: сб. науч.тр. / редкол.: В.Н. Бибило (гл. ред.) [и др.]. – Минск: БГУ, 2007. – Вып. 18. – С. 239–249.

3. Лепехин, А.Н. Криминалистическое обеспечение расследования преступлений против информационной безопасности: автореф. дис. … кандид. юрид. наук : 12.00.09 / А. Н. Лепехин ; Академия МВД Республики Беларусь. – Минск, 2007. – 21 с.

4. Лосев, В.В. Уголовно-правовой анализ преступлений против информационной безопасности / В.В. Лосев // Судовы веснік. – 2003. – № 4. – С. 18–22.

5. Шидловский, А.В. О направлениях дифференциации уголовной ответственности за кибертеррооризм и иные киберпосягательства / А.В. Шидловский // Право.by. – 2018. – 1(51). – С. 86–9.

УДК 004:338.22

Г.В. Кораблева, С.М. Морозов
Московский государственный университет
технологий и управления имени К.Г. Разумовского (ПКУ)

РАСШИРЕНИЕ СФЕР ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

В ФГБОУ ВО «Московский государственный университет технологий и управления имени К.Г. Разумовского (ПКУ)» ведётся подготовка бакалавров по направлению «Информатика и вычислительная техника», они формируют кадровый потенциал государства в условиях цифровой экономики. Если пять и более лет назад выбор тем выпускных квалификационных работ для студентов этого направления подготовки не составлял большого труда, то сейчас, анализируя области применения информационных технологий и типовые программные решения российских и зарубежных разработчиков, автоматизирующих бизнес-процессы в государственных организациях, на коммерческих предприятиях, в банковской сфере, в маркетинге и торговле, а также ряде других прикладных областей, всё труднее найти задачи, для решения которых пока не разработаны типовые программные продукты.

На российском рынке программного обеспечения в настоящее время достаточное количество автоматизированных ERP-систем, CRM-систем, программ для ведения бухгалтерского и финансового учёта, учёта кадров и управления персоналом, планирования и управления производством, ведения электронного документооборота, информационных правовых справочных систем.

Чтобы не дублировать типовые программные решения при выполнении студентами проектов и выпускных квалификационных работ в качестве тем выдаются для разработки специализированные web-приложения, мобильные приложения либо автоматизированные системы поддержки принятия решений для решения нестандартных задач конкретных заказчиков. Также актуальна разработка и внедрение