действие только трудовое законодательство. С 2009 г. заработная плата осужденных составляет 9 % от оплаты труда обычного работника [3, с. 81]. В случае если осужденный выполняет тяжелые работы либо работы с опасными условиями труда, то ему выплачиваются определенные законом доплаты.

Особенностью организации общественно полезного труда в Норвегии является тот факт, что при получении осужденными образования любой формы, они не привлекаются к обязательным работам. Кроме этого, правительство страны устанавливает минимальный и максимальный размеры оплаты труда.

В Финляндии рабочий день осужденных составляет 40 часов в неделю, суббота и воскресенье являются выходными днями, как и у всех граждан страны. Труд осужденных в закрытых тюрьмах оценивается незначительной строго фиксированной суммой, но из нее не удерживаются налоги. Вместе с тем, в открытых заведениях осужденные получают заработную плату сравнимую с той, которую получают работники в условиях свободы.

Таким образом, можно сделать вывод, что независимо от экономического развития страны, процесс организации труда осужденных вызывает определенные трудности. Опираясь на опыт зарубежных стран, в национальную практику организации общественно полезного труда постепенно могут вноситься следующие изменения: установление минимального и максимального размера заработной платы осужденных; заключение трудовых договоров с осужденными, переведенными на более мягкие условия отбывания наказания; сокращение часов привлечения к неоплачиваемому труду; сокращение часов рабочего дня в случае получения осужденным образования; привлечение частного сектора к организации труда в ИУ. Улучшение условий и качества общественно полезного труда в ИУ будет содействовать повышению эффективности успешной ресоциализации осужденных в условиях свободы.

Список литературы

1. Шабанов, В. Б. О правовом регулировании труда осужденных к лишению свободы: проблемы и перспективы / В. Б. Шабанов, О. М. Савастей // Вестник Академии МВД Республики Беларусь. – 2019. – № 2 (38). – С. 162 – 166.

2. Антонян Е. А. Привлечение осужденных к труду за рубежом [Электронный ресурс] // Человек: преступление и наказание. – Режим доступа: https://cyberleninka.ru/article/n/privlechenie-osuzhdennyh-k-trudu-za-rubezhom/viewer. – Дата доступа: 03.12.2020.

3. Шилова, Н. П. Особенности труда лиц, осужденных к лишению свободы / Н. П. Шилова // Пенитенциарная наука. – 2009. – № 1. – С. 78–84.

А.И. Балабкина
МГУ им. А.А. Кулешова (Могилёв)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Информация – одно из основополагающих понятий современного бытия и относится к категории тех, которые имеют очень широкий спектр применения.

Законодательством об информации, информатизации и защите информации выделяется термин «информация» как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Существенный анализ основ информационной безопасности показал, что обеспечение режима информационной безопасности – задача крайне сложная и комплексная. По первому мнению, информационная безопасность предполагает безопасность как минимум трех ее составляющих – доступность, целостность и конфиденциальность существующих данных. Исходя из этого, вопрос информационной безопасности требует всестороннего рассмотрения. По второму мнению, информация и информационные системы буквально «проникают» во все сферы общественной деятельности и влияние информации на общество возрастает, поэтому обеспечение информационной безопасности также требует всестороннего подхода. Термин «информационная безопасность» может иметь различные толкования в зависимости от предлагаемого контекста. Информационная безопасность также должна означать безопасность информации и поддержание инфраструктуры от случайных или преднамеренных воздействий различного характера, которые могут нанести невосполнимый ущерб субъектам информации, включая владельцев и пользователей информации.

В различных источниках вводится понятие информационной безопасности как состояния защищенности информации, при котором обеспечены ее *конфиденциальность* – требование не допускать распространения и (или) предоставления информации без согласия ее носителя, *доступность* – состояние информации, при котором субъекты, имеющие на законных основаниях доступ к ней реализуют его беспрепятственно и *целостность* – информация, при различных операциях с ней (передача, хранение или представление) не была изменена.

Информация становится предметом общественных отношений, начинает приобретать товарные свойства и становится предметом купли-продажи. Итогом информационных процессов является формирование новых общественных отношений и видоизменение существующих. В современном мире можно зафиксировать большое количество договорных отношений, связанных с производством, передачей, сбором и использованием информации в различных формах [1, с. 78].

Широкое развитие информационных технологий привело к модификации старых и появлению совершенно новых форм и видов преступлений, связанных с использованием информации и различных информационных систем.

На сегодняшний день, по данным Организации объединенных наций, ущерб, наносимый преступлениями в сфере информационных технологий, сопоставим с доходами от незаконного оборота оружия и наркотиков. Только в Соединенных штатах Америки ущерб ежегодно составляет 100 миллиардов долларов. Конечно, подобного рода преступления в Республике Беларусьеще не достигли такого масштаба, но наука и технологии развиваются все быстрее и быстрее, и у преступников появляется все больше новейших способов осуществления своих незаконных замыслов.

Информационная сфера выделяется как одна из сфер, где сосредоточены усилия и ресурсы для обеспечения национальной безопасности. Она активно влияет на состояние политической, экономической, военной и других направлений национальной безопасности Республики Беларусь. Национальная безопасность страны в принципе

зависит от обеспечения информационной безопасности, и эта зависимость будет усиливаться по мере технического прогресса.

Преступления против информационной безопасности совершаются различными лицами (как специалистами в сфере информационных технологий, так и обычными пользователями, не обладающими специальными навыками), при этом мотив преступного деяния также может быть совершенно разным.

Преступление против информационной безопасности – это запрещенное уголовным законом Республики Беларусь общественно опасное виновное деяние, посягающее на безопасность информационных процессов в части сбора, обработки, накопления, хранения, поиска, распространения, информации с помощью компьютерных систем или сетей.

Уголовный Кодекс Республики Беларусь к категории преступлений против информационной безопасности относит: несанкционированный доступ к компьютерной информации, неправомерное завладение и модификацию компьютерной информации, компьютерный саботаж, изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети, разработку, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети, нарушение тайны переписки или иных сообщений, хищение путем использования компьютерной техники [2, с. 57].

Технологии развиваются настолько быстро и стремительно, а методы совершения преступлений настолько изощрены, что зачастую это приводит к невозможности собирания всех необходимых доказательств к совершенному преступлению. В результате это может привести к привлечению невиновных лиц к ответственности.

Совершая вышеуказанные преступления, лицо напрямую не осуществляет завладение имуществом, однако в тоже время, своими действиями оно наносит значительный вред охраняемым законом правам и интересам.

В настоящее время решающим фактором для обеспечения информационной безопасности Республики Беларусь является активное внедрение информационно-телекоммуникационных технологий на основе компьютерной техники во все сферы жизнедеятельности общества, особенно в республиканские органы государственного управления и кредитно-финансовую сферу, представляющие собой совокупность программных, технических и организационно-экономических средств, объединенных структурно и функционально объединены для решения задач передачи и обработки информации.

Дальнейшее развитие законодательства Республики Беларусь в области информационной безопасности должно основываться на соблюдении баланса между интересами личности, общества и государства и их взаимной ответственности, интеграции в рамках международной информационной безопасности. Современное белорусское правовое обеспечение информационной безопасности перед лицом новых угроз должно осуществляться через современные методологические подходы к правовому регулированию во всех отраслях права.

Создание системы безопасности – важнейшее звено в последовательном ряде принимаемых решений в сфере информационной безопасности. Первой и наиболее важной проблемой при создании системы информационной безопасности является

оценка требований по безопасности, а также идентификация критичных по безопасности информационных ресурсов защищаемой информационной системы. В частности, в качестве перспективного механизма обеспечения кибербезопасности планируется создание единой системы мониторинга белорусского интернет-сегмента, объединяющей национальный центр и сеть ведомственных (производственных) центров по выявлению и борьбе с угрозами и инцидентами информационной безопасности (SOC).

Приоритетным направлением является совершенствование нормативно-правовой базы для обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе за счет оптимизации механизмов государственного регулирования в данной сфере. При этом большое значение придается выстраиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

Список литературы

1. Лапина, М.А. Информационное право: Учеб. пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / М.А. Лапина, А.Г.Ревин, В.И. Лапин; Под ред. проф. И.Ш. Килясханова. – М.: ЮНИТИ-ДАНА, Закон и право, 2004. – 335 с.

2. Лепехин, А. Преступления против информационной безопасности: правовые аспекты / А. Лепехин // Судовы Веснік. – 2006. – № 1. – С. 57–59.

Л.В. Бойченко
Академия управления при Президенте Республики Беларусь (Минск)

ДЕЛОВАЯ РЕПУТАЦИЯ: ПОНЯТИЕ И ОСОБЕННОСТИ ЗАЩИТЫ

Положительная деловая репутация играла и продолжает играть ключевую роль для любой организации, индивидуального предпринимателя или гражданина в аспекте их экономического успеха. Как таковая, деловая репутация формируется в процессе взаимодействия какого-либо участника гражданского оборота с иным субъектом и формируемого на основания этого взаимодействия конкретного представления о его деловых качествах.

Что касается понятия «деловой репутации», то законодатель Республики Беларусь не дает ему четкого юридического определения. В п. 7 ст. 153 Гражданского кодекса Республики Беларусь (далее – ГК) закрепляется возможность защитить деловую репутацию организации через суд. Однако данная норма не позволяет выделить, что же понимается под деловой репутацией [1].

Экономические суды придерживаются точки зрения, согласно которой деловая репутация представляет собой оценку участника отношений в сфере предпринимательской и иной хозяйственной (экономической) деятельности другими участниками (п. 1 постановления Пленума Высшего Хозяйственного суда (далее – ППВХС №16)) [3].