государственной поддержки последовательно сокращается: с 2,8 млрд р. в 2016 г. – до 0,8 млрд р. в 2019 г. Нельзя не учитывать также, что на ряде предприятий используется устаревшее оборудование, что, безусловно, является серьезной угрозой для их стабильного, устойчивого развития. Исключительно важно в усложняющихся экономических условиях своевременно выработать меры, направленные на укрепление существующих гарантий и повышение эффективности механизмов защиты прав работников в случае экономической несостоятельности (банкротства) организаций, бережно относиться к имеющемуся трудовому потенциалу. Как эта задача решается в других странах?

Поскольку банкротство является неотъемлемым элементом рыночной экономики, в разных странах применяются различающиеся модели защиты прав трудящихся при ликвидации предприятия, экономической несостоятельности (банкротстве) работодателя. Так, например, в Бразилии, Колумбии, Малайзии, Чили осуществляется полное страхование от безработицы, позволяющее работнику получить возмещение в зависимости от минимального размера оплаты труда за определенный период (как правило до 2 лет), кроме того, работникам обеспечивается возможность скорейшего трудоустройства на основе повышения их профессиональной мобильности. В Германии используется другой подход. Здесь требования работников, неудовлетворенные в рамках процедуры конкурсного производства, возмещаются за счет Национального фонда страхования на случай банкротства работодателя. В других европейских странах применяется иная модель. Необходимые выплаты работникам, связанные с трудовыми отношениями, в случае ликвидации организации по причине экономической несостоятельности (банкротства) возмещаются страховыми фондами в полном объеме.

В Конвенции Международной организации труда № 173 (от 23 июня 1992 г.) «О защите требований трудящихся, в случае неплатежеспособности предпринимателя» предусмотрено создание специальных гарантийных учреждений.

Применяемый в нашей стране механизм компенсации потерь наемным работникам в случае ликвидации, экономической несостоятельности (банкротства) нанимателя требует совершенствования.

Изучение международного опыта и возможностей его применения в Беларуси позволяет сделать вывод о целесообразности введения обязательного страхования на случай утраты заработка вследствие ликвидации, экономической несостоятельности (банкротства) нанимателя. Целесообразно создать специальный целевой фонд, который финансируется за счет взносов всех субъектов хозяйствования. Такой фонд является практической формой реализации социальной ответственности бизнеса и обеспечит значимую поддержку наемных работников в случае ликвидации, экономической несостоятельности (банкротства) нанимателя.

Защита законных интересов и прав работников в ходе модернизации национальной экономики – один из ключевых факторов обеспечения экономической безопасности государства.

УДК 004:34

В.С. Божков

ТЕХНОЛОГИЧЕСКИЕ ТРЕНДЫ И УГРОЗЫ: ПРОБЛЕМЫ И ИХ РЕШЕНИЕ

Одним из негативных последствий развития современных информационных технологий является появление и развитие новой формы преступности – в сфере высоких технологий. Проблема киберпреступности становится все более острой в эпоху информационного общества, когда информационные технологии охватывают все сферы жизнедеятельности граждан и государства. Жертвами преступников в киберпространстве могут стать не только люди, но и предприятия, города, страны.

В современном мире киберпространство, как правило, не знает государственных границ. В числе наиболее актуальных угроз, которым необходимо противодействовать в настоящее время, следует назвать: атаки бизнес-структур программами-вымогателями; использование социальной инженерии с целью хищения денежных средств с карт-счетов граждан; нарастающий рынок продажи персональных данных; рост количества вредоносных программ для мобильных устройств; использование средств фальсификации – голоса, сообщений, цифровых событий; распространение готовых инструментов для кибератак (вымогательское ПО как услуга); использование кибероружия.

Определенные риски нарастают по мере ускорения темпов внедрения проектов и технологий «умного города». Экосистема «умных городов» включает в себя следующие слои: физические устройства и оборудование, ядро или платформу сбора данных, коммуникационные каналы. Ключевыми факторами, создающими киберугрозы в городах, являются:

объединение физических и цифровых инфраструктур;

одновременное использование новых и устаревших решений;

интеграция, смешение данных и сервисов различных городских структур и служб.

Сближение информационных систем и операционных инфраструктур не только позволяет городским службам удаленно собирать данные и управлять техническими системами благодаря цифровым инструментам и решениям, но также существенно увеличивает риски и пространство для новых угроз. Проблемы и уязвимости одних сервисов могут быстро каскадироваться на множество связанных систем.

К ключевым компонентам интегрированного подхода к построению кибербезопасности современных городов, по нашему мнению, могут быть отнесены:

защищенная цифровая платформа, которая обеспечивает защищенные соединения, управляет идентификацией и связями в подключенной экосистеме. Примеры достаточно надежных решений – защищенные чипы и микроэлектронные компоненты, позволяющие идентифицировать конкретное устройство и исключить возможность его неправомерного использования;

конфиденциальность персональных данных – подход призван защитить неприкосновенность данных граждан посредством соответствующей архитектуры решений, выбором технологий, процессов, инфраструктуры. Ориентир – это те решения, в которых гражданин является владельцем собственных данных и вправе контролировать доступ к ним (например, банковские и медицинские данные);

сводная платформа анализа и обнаружения киберугроз, которая нацелена на поиск и выявление угроз благодаря работе со множеством городских и ведомственных баз данных, событий, фактического материала. Используя аналитику больших данных, машинное обучение, такая платформа позволяет формировать целостную картину пространства угроз с целью обеспечения правоохранительных органов возможностями сценарного планирования для профилактики различных правонарушений и более оперативного обнаружения и реагирования;

ответ на угрозы и устойчивость к атакам – подготовка, моделирование и проигрывание потенциальных сценариев позволят городам увеличить скорость реагирования и готовить превентивные ответные меры защиты. Устойчивые решения позволяют исключить сбои и отключения связных и высокоуровневых систем по причинам инцидентов на уровне отдельных систем или устройств;

повышение цифровой грамотности и экспертизы в вопросах цифровой безопасности – усложнение и цифровизация городских инфраструктур вызывает необходимость дополнительной и регулярной подготовки сотрудников и руководителей большого перечня ведомств и служб в вопросах кибербезопасности на уровнях физических устройств – персональных и технологических, цифровых баз данных, каналов коммуникаций, цифровых приложений;

согласованная стратегия реализации проектов «умного города» и кибербезопасности. Разрозненные структуры и ведомства с собственными подходами, базами данных, платформами и аналитикой необходимо объединять общими целями, приоритетами и метриками исходя из комплексного подхода к управлению угрозами и рисками, с пониманием взаимосвязей и зависимостей данных, процессов, событий – с возможностями профилактики, предотвращения, обнаружения и реагирования;

формализация согласованного сбора, хранения и управления данными, активами, инфраструктурами и различными технологическими компонентами. Согласованное взаимодействие и работа различных городских структур, ведомств, предприятий позволят объединять возможности по обнаружению, аналитике, профилактике и реагированию на различные угрозы. Важно отметить необходимость построения процессов регулярной интеграции и усиления согласованности взаимодействия городских служб с учетом постоянного усложнения самой городской экосистемы, с одной стороны, ускорения и усложнения цифровизации преступности – с другой;

построение стратегических партнерств и согласованного взаимодействия на различных уровнях цифровой экосистемы города. Это цифровизация на уровне включения физических объектов в цифровую среду, коммуникационные средства и инфраструктуры, базы данных служб и предприятий, цифровые платформы и приложения – цели, средства, программы модернизации и развития.

УДК 343.985

С.И. Бординович

НЕКОТОРЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «КОНТРОЛИРУЕМАЯ ПОСТАВКА»

Проведение оперативно-розыскного мероприятия «контролируемая поставка» (далее – контролируемая поставка), представляющего собой перемещение гражданином, организацией предметов и документов под контролем должностного лица органа, осуществляющего оперативно-розыскную деятельность (ОРД), в целях получения сведений, необходимых для выполнения задач ОРД, как правило, требует комплексного задействования сил и средств различных государственных органов, организаций, а также граждан, оказывающих содействие на конфиденциальной основе органам, осуществляющим ОРД, посредством участия в проведении указанного оперативно-розыскного мероприятия, содействия в его подготовке и проведении.

В ходе проведения контролируемой поставки осуществляется установление каналов поступления запрещенных к обороту веществ и предметов. Наряду с этим решается задача по установлению их отправителей и получателей, а также лиц, совершивших или совершающих преступления с использованием контролируемых предметов и документов. Для выявления и закрепления доказательства преступной деятельности создаются условия, при которых следы совершаемого преступления отражаются на допускаемых уголовно-процессуальным законом носителях информации.

Согласно Закону Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» контролируемая поставка проводится по постановлению о проведении оперативно-розыскного мероприятия и в рамках дела оперативного учета, представляющего собой обособленное производство, которое включает в себя материалы ОРД в целях систематизации, проверки и оценки сведений, оно заводится по постановлению должностного лица органа, осуществляющего ОРД. Еще одним обязательным условием проведения контролируемой поставки является наличие специального задания, которое объявляется под подпись гражданину, привлекаемому к участию в оперативно-розыскном мероприятии, до начала его проведения.

При проведении контролируемой поставки законодательство допускает полное или частичное изъятие, а также замену перемещаемых вещей, оборот которых представляет повышенную опасность для здоровья граждан и окружающей среды или служащих для изготовления оружия массового поражения.