опасности (ОДКБ), Шанхайская организация сотрудничества (ШОС) и Евразийское экономическое сообщество (ЕАЭС), которые неоднократно высказывали свою приверженность в деле сотрудничества в противодействии торговле людьми.

УДК 343.8

О.Г. Ковалев

МОДЕЛИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ РАЗВИТЫХ ЗАРУБЕЖНЫХ СТРАН НА СОВРЕМЕННОМ ЭТАПЕ

Проблема современной кибербезопасности в условиях постоянно меняющегося и развивающегося киберпространства, роста киберпреступности, распространения киберугроз, совершения несанкционированных, криминальных кибератак на различные государственные учреждения, коммерческие организации, структуры и компании, факты кибертерроризма требуют обеспечения кибербезопасности на современном, высоком уровне.

За последние шесть лет киберпреступность в Российской Федерации выросла в 10 раз, ущерб от нее оценивается до 3 трлн р. Каждое пятое регистрируемое преступление совершается с использованием компьютерных технологий. По оценкам экспертов, латентность в сфере digital-преступности доходит до 85 %. Киберпреступники, атакующие государственные, финансовые учреждения, оборонные, ресурсодобывающие, медицинские, туристические и другие компании и персональных пользователей, применяют разнообразные современные IT-технологии и программное обеспечение.

В настоящее время кибербезопасность в Российской Федерации обеспечивают Генпрокуратура, МВД, СК, ФСБ, Минобороны, ФСО, Росгвардия и Минюст России.

В связи с актуальностью данного вопроса нами проводятся комплексные теоретико-эмпирические исследования правовых и организационных проблем обеспечения кибербезопасности, в том числе в правоохранительной, оборонной, банковской сферах, в уголовно-исполнительной системе.

Только в текущем году, по результатам исследований, опубликованы около 10 научных статей в различных изданиях, в том числе журналах, рецензируемых ВАК при Минобрнауки России (Воен.-юрид. журн. 2021. № 3).

Одним из промежуточных результатов изучения проблемы стало понимание киберпреступности как угрозы национальной безопасности современной России, необходимости выработки единой стратегии комплексного и системного противодействия киберугрозам, нормативно-правового регулирования, предупреждения и своевременного, адекватного реагирования на возникающие киберинциденты различной степени сложности со стороны специальных государственных органов, общественных организаций, бизнес-сообществ и граждан. Требуется также создание современной организационной структуры обеспечения кибербезопасности, в том числе на объектах, наиболее подверженных риску кибератак со стороны киберпреступников и криминальных киберсообществ, ее первоочередное финансирование, кадровое, техническое и научное обеспечение.

В этих целях может быть полезен опыт развитых зарубежных стран, которые уже длительное время и весьма эффективно противодействуют киберпреступности, обеспечивают кибербезопасность на высоком профессиональном уровне.

В результате осуществленного теоретического изучения различных подходов, распространенных в зарубежных государствах, методами сравнительного и контент-анализа нами были выявлены и описаны основные модели организации кибербезопасности. При этом использовались географический и организационно-экономический принципы обобщения и классификации полученных результатов.

Так называемая североамериканская модель организации кибербезопасности, которую используют США и Канада, начала активно развиваться после террористических атак 11 сентября 2001 г., показавших уязвимость системы национальной безопасности США, ее неспособность предотвращать современные угрозы и реагировать на них. В помощь уже существовавшим субъектам кибербезопасности (ФБР, ЦРУ, Министерство обороны, полиция, организации разведывательного сообщества) в кратчайшие сроки было создано Управление внутренней безопасности, статус которого в скором времени был повышен до профильного министерства.

Отличительной чертой рассматриваемой модели является модернизация и создание новых организационных структур, подведомственных различным государственным правоохранительным, военным и разведывательным ведомствам, обменивающихся информацией о крупных киберинцидентах, координирующих совместную деятельность и финансируемых федеральным правительством.

Так, созданное в 2018 г. Агентство по кибербезопасности и безопасности инфраструктуры активно взаимодействует с Министерством

юстиции, входящими в него ФБР и Национальной объединенной рабочей группой по киберрасследованиям.

Министерство внутренней безопасности противодействует киберугрозам, разрешает киберинциденты с помощью Национального центра интеграции кибербезопасности и связи.

Управление директора национальной разведки, используя возможности Центра интеграции информации о киберугрозах, является главным федеральным органом их разведывательного обеспечения, сопровождения и нейтрализации.

Европейская модель направлена на реализацию утвержденной странами Европейского союза стратегии обеспечения кибербезопасности, осуществляемой на союзном и государственном уровнях. Данная модель отличается более продуманным и организованным комплексом мероприятий, проводимых в рассматриваемом контексте (разработка концепции киберустойчивости организаций и объектов к киберинцидентам различного содержания, длительности и интенсивности, законодательное, организационное, методическое, материально-техническое, кадровое и финансовое сопровождение).

Активно осуществляется формирование в сознании граждан культуры кибербезопасности, алгоритмизации реагирования пользователей Сети на возможные ухищрения, используемые киберпреступниками (фишинговые письма, программы-шифровальщики, программные вирусы и др.). В этих целях проводится системная разъяснительная работа, так называемые ежегодные месячники кибербезопасности, повышающие уровень знаний и навыков должностных лиц и граждан в сфере кибербезопасности.

Обеспечением кибербезопасности в соответствии с принятым в 2019 г. специальным законом занимаются не только специализированные государственные структуры в сфере IT-технологий (Агентство Европейского союза по сетевой и информационной безопасности, осуществляющее информационно-аналитические и практические мероприятия по предупреждению, выявлению и разрешению киберинцидентов), но и общественные организации, онлайн-сообщества, бизнес-структуры, исследовательские и образовательные учреждения.

Зарекомендовал себя с положительной стороны созданный восемь лет назад Европейский центр борьбы с киберпреступностью, внесший значительный вклад в борьбу с этим криминальным явлением, его резонансными проявлениями на территории государств Евросоюза.

Следует обратить особое внимание на вопросы материально-технического обеспечения реализации стратегии кибербезопасности государств Европейского союза в постпандемийный период, а также их финансирования, исчисляемого почти 2 млрд евро.

В ходе исследования нами также определены другие модели обеспечения кибербезопасности: китайская (КНР), стран Юго-Восточной Азии (Южная Корея, Сингапур, Индонезия и Малайзия), а также государств, ориентированных на национальный, государственный интернет (Иран, КНДР).

Таким образом, рассмотренные основные модели свидетельствуют об озабоченности и приоритетности деятельности органов законодательной и исполнительной власти различных государств, институтов гражданского общества и бизнеса по созданию, внедрению и развитию современных форм и методов противодействия киберпреступности, обеспечения кибербезопасности.

УДК 343.985

А.А. Ковальчук

О ВЗАИМОДЕЙСТВИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И ПРЕДСТАВИТЕЛЕЙ БАНКОВСКОГО СЕКТОРА В КОНТЕКСТЕ БОРЬБЫ С ХИЩЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК И ИХ РЕКВИЗИТОВ

Официальная статистика МВД Республики Беларусь показывает, что в 2020 г., как и в предыдущие годы, растет количество хищений, совершенных путем использования компьютерной техники (ст. 212 УК Республики Беларусь). Значительную часть среди них составляют хищения, совершенные с использованием реквизитов банковских платежных карточек (БПК). Для завладения реквизитами злоумышленники чаще всего используют методы социальной инженерии посредством телефонных и интернет-коммуникаций, а также так называемые фишинговые интернет-ресурсы.

Возможность совершения хищений в ряде случаев обусловлена неосмотрительностью со стороны держателей БПК. Невзирая на комплекс профилактических мероприятий, проводимых ГУПК КМ МВД Республики Беларусь в средствах массовой информации, в том числе в сети Интернет, держатели БПК продолжают допускать ошибки, приводящие в дальнейшем к совершению хищений.

Указанное требует от представителей банковского сектора принятия соответствующих мер реагирования, направленных на усиление защиты клиентов банков от противоправных посягательств. В этой связи ГУПК КМ МВД на основе всестороннего изучения существующих проблем подготовлен актуальный комплекс мер, включающий: