представителя) воспользовался некий сотрудник, не имея на то согласия уполномоченного лица, либо отдельные условия договора согласовывало не уполномоченное, а иное лицо, которое воспользовалось аналогом собственноручной подписи руководителя (уполномоченного представителя), не имея на то согласия уполномоченного лица.

К тому же, как показывает судебная практика, часто суд не принимает договор, заключенный в электронном виде, требуя его бумажный вариант. Сложности возникают и внутри государственных организаций, поскольку, например, бухгалтерия также требует бумажный вариант заключенного на электронной торговой площадке договора как доказательство того, что он подписан обеими сторонами и имеет юридическую силу.

Таким образом, в правовом регулировании в сфере государственных закупок, в реализации отдельных норм и положений Закона, других нормативных правовых актов имеются проблемы, которые отрицательно влияют на экономику отдельных государственных предприятий и страны в целом. Вместе с тем государственные закупки представляют собой эффективный инструмент обеспечения экономической безопасности государства. Внедрение в Республике Беларусь «электронного государства» требует решения ряда проблем, возникающих в ходе реализации существующих норм и положений. Информационное общество, несмотря на определенные трудности, стремится к простому, быстрому и комфортному взаимодействию с государством и, в свою очередь, помогает государству решать различные проблемы и задачи, т. е. повышать благосостояние нации.

УДК 004.056

С.Ю. Воробьёв, Д.А. Жук, В.А. Русак, В.А. Шкред

ОСОБЕННОСТИ КИБЕРПРЕСТУПЛЕНИЙ В БАНКОВСКОМ СЕКТОРЕ

В эпоху стремительного развития технологий практически все сферы жизнедеятельности человека подверглись цифровой трансформации. Появились такие правонарушения, которые получили общее название «киберпреступность». Кража данных доступа к системе интернет-банкинга, а также банковских платежных карточек (банковских счетов) с целью завладения средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникации с целью создания убытков компаниям – часть подобных угроз, связанных с бурным развитием информационных технологий.

Опасность киберпреступлений в банковском секторе связана с тем, что цифровые технологии развиваются стремительно и злоумышленники изобретают новые способы обхода систем безопасности, к которым имеющиеся системы защиты не готовы. Киберпреступления, как и другие виды преступлений, совершаются одним или несколькими правонарушителями, как правило, обладающими колоссальными знаниями в области цифровых технологий, используемыми для достижения корыстных целей. Наиболее привлекательным для таких преступников является банковский сектор, в котором ежедневно происходит множество транзакций и осуществляется оборот огромного количества денежных средств.

Так, в поле зрения злоумышленников и международных преступных группировок находится банковская система Республики Беларусь. В последние несколько лет постоянно выявлялись факты мошенничества с использованием электронных платежных средств, имели места хакерские атаки на банки Республики Беларусь, в результате которых злоумышленники похищали значительные денежные средства. Сотрудниками правоохранительных органов на территории Республики Беларусь задерживались участники международных преступных группировок Cobalt, Andromeda и др.

Анализ мировой практики правоохранительной деятельности позволяет выделить следующие наиболее характерные для банковской сферы виды киберугроз:

воздействие через аппаратные уязвимости, которые имеются в микропроцессорах разных производителей и не устраняются при помощи программных обновлений, но открывают новые возможности для злоумышленников;

компьютерный шпионаж, направленный на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и слежения за деятельностью финансовых организаций;

целенаправленные кибератаки на конкретные финансовые организации, позволяющие злоумышленникам проникать в сеть организаций и далее к изолированным финансовым системам для вывода денежных средств;

клиентоориентированные кибератаки, направленные непосредственно на клиентов банков, а именно на хищение их денежных средств.

Типовая схема таргетированной кибератаки на банк состоит из следующих этапов:

массовая рассылка писем на e-mail работников банка, в которых содержится вредоносное программное обеспечение;

внедрение вредоносного программного обеспечения при открытии письма работником банка для установки доступа к зараженному компьютеру;

исследование доступных с зараженного компьютера сегментов локальной сети банка и установка доступа к контроллеру домена с целью получения паролей администраторов сети;

поиск в сети финансового учреждения представляющих интерес рабочих станций и серверов, в первую очередь компьютера или сервера с доступом в подсеть, в которой находятся банкоматы или иные сегменты сети, например в сегмент процессинга банковских платежных карточек;

установка на банкоматах вредоносного программного обеспечения для выдачи финансовой наличности посредством удаленной команды.

После установления контроля над банкоматом к процессу подключаются соучастники, задача которых – непосредственное присутствие у подконтрольного банкомата в условленное время для получения денег. После успешного изъятия наличности вредоносное программное обеспечение, как правило, с банкоматов деинсталлируется.

Большинство вредоносных программ создаются и распространяются в целях получения несанкционированного доступа к финансовым системам для хищения учетных данных пользователей, рассылки спама, шифрования жестких данных на диске с последующим вымогательством денежных средств за расшифровку.

Необходимо упомянуть и о такой деятельности злоумышленников, как социальная инженерия, – одной из главных угроз кибербезопасности.

Представляется возможным выделить ряд особенностей, присущих правонарушениям в банковской сфере с применением информационных технологий: применение компьютерной техники, высокая латентность, умышленная корыстная направленность, высокая степень организованности.

В связи с тем что банковские и иные финансовые учреждения принимают меры для защиты своей инфраструктуры, а также финансов и транзакций клиентов, киберпреступники постоянно повышают свою квалификацию.

Для успешного предотвращения кибератак на банковский сектор необходимо принятие финансовыми учреждениями следующих мер:

использование соответствующих аппаратных, программных и программно-аппаратных комплексов средств защиты информации;

мониторинг событий безопасности;

постоянное повышение квалификации работников, отвечающих за информационную безопасность;

обучение работников банков основам информационной безопасности;

поддержание здорового климата в коллективе, поскольку не имеющий претензий работник с меньшей долей вероятности осознанно навредит организации, в которой работает;

информирование клиентов банков и обучение их финансовой и цифровой грамотности;

разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке;

создание команды по расследованию инцидентов информационной безопасности;

скрупулезный подбор персонала в банковские организации с учетом профессиональных, нравственных и моральных качеств специалистов;

взаимодействие банков, правоохранительных органов и организаций, осуществляющих помощь в борьбе с киберугрозами.

УДК 346.7

В.С. Гальцов

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-ТОРГОВЛИ КАК НАПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ

Цифровая экономика – система социальных, экономических и технологических отношений между государством, бизнес-сообществом и гражданами, функционирующая в глобальном информационном пространстве посредством широкого использования цифровых информационно-коммуникационных технологий (ИКТ), генерирующая цифровые виды и формы производства и продвижения к потребителю продукции и услуг, которые приводят к непрерывным инновационным изменениям методов управления и технологий в целях повышения эффективности социально-экономических процессов (Головенчик Г.Г. Цифровизация белорусской экономики в современных условиях глобализации. Минск, 2019. С. 30).

Понятие «цифровая экономика» имеет несколько аспектов. Она рассматривается:

на государственном уровне как экономическая политика, целью которой является повышение эффективности за счет перехода государственного управления и экономических отношений на цифровую основу, т. е. цифровая экономика = национальная экономика + ИКТ.

на отдельных предприятиях как использование ИКТ для автоматизации хозяйственной деятельности, создания или реализации продукции (например, интернет-торговля);

в обществе как использование автоматизированных информационных систем для обеспечения жизнедеятельности и для потребления