ный криптографический протокол аутентификации, включающий, например, вычисление цифровой подписи. В процессе аутентификации используются протоколы с защитой данных.

В настоящее время в торговле набирает популярность мобильный SoftPOS-эквайринг. Он дает возможность принимать безналичные платежи с помощью смартфона с NFC-модулем (Near Field Communication). Для покупателя процесс оплаты выглядит аналогично покупке при помощи обычного платежного терминала. Он прикладывает свою бесконтактную карточку к смартфону продавца, на котором установлено приложение SoftPOS-эквайринга. После обработки платежа у продавца на экране телефона отображается информация об успешно проведенной операции, а покупатель получает оплаченный товар или услугу. Электронный чек приходит в виде SMS.

Адаптация функционала SoftPOS-эквайринга к переводам с карточки на карточку (P2P-переводам) позволит продавцу выставлять электронный счет, а покупателю акцептовать его, приложив свою карточку к смартфону.

Для дистанционных сделок возможным решением является интернет-эквайринг. В процессе оформления приобретаемого товара или услуги покупатель покидает сайт продавца и перенаправляется на специальный защищенный сайт банка-эквайера, что можно сразу заметить в адресной строке браузера. При оплате покупок в интернете вместо терминала используется специальный защищенный сервис банка.

Организация платежного сервиса на электронных торговых площадках имеет ряд положительных факторов и для торговой площадки, и для продавцов, и для покупателей. Средства покупателя депонируются на счете торговой площадки до получения от покупателя подтверждения о соответствии товара заявленному в объявлении о продаже, после чего перечисляются продавцу. На счетах торговой площадки формируется оборотный капитал, что создает источник средств для инвестирования и дополнительного дохода. Продавец сообщает сведения о своей банковской платежной карточке только торговой площадке, что защищает его от социальной инженерии мошенников на стороне покупателя. Покупатель приобретает дополнительную защиту своих прав. В случае получения товара ненадлежащего качества он имеет возможность расторгнуть сделку, вернуть товар продавцу и вернуть удерживаемую торговой площадкой уплаченную сумму.

Менее технологичным и менее защищенным вариантом является информационное взаимодействие электронной торговой площадки с банковскими сервисами переводов с карточки на карточку (P2P-переводы). Идея заключается в создании возможности сторонам сделки перейти с сайта торговой площадки на страницу банка эмитента

карточки покупателя с официальной информацией об условиях перевода с карточки на карточку.

Таким образом, дальнейшее развитие используемых и создание новых сервисов безналичной оплаты товаров и услуг для физических лиц позволит отказаться от использования CVV/CVC кодов и создать механизм противодействия кибермошенничеству с применением социальной инженерии.

УДК 340.1

К.В. Янчуревич

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КАК ВАЖНЫЙ ЭЛЕМЕНТ ПРОЦЕССА ФОРМИРОВАНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РЕСПУБЛИКЕ БЕЛАРУСЬ

В настоящее время в ряде стран наблюдается процесс активного формирования и развития информационного общества. В зависимости от множества различных факторов отдельные государства находятся на разных этапах вышеуказанного процесса.

Следует отметить, что информационное общество представляет собой сложную систему, которая включает в себя множество элементов. Большинство ученых, занимавшихся исследованиями в области информационного общества, сходятся во мнении, что именно информация, по сути, и является центральным звеном («ядром») информационного общества.

Необходимо подчеркнуть, что для того чтобы общество могло беспрепятственно пользоваться информацией, распространять ее, а также ощущать защищенность от преступных посягательств со стороны преступников, следует применять высокоэффективные действенные меры.

Безусловно, уже разработано и активно применяется на практике достаточно много способов борьбы с киберпреступлениями (правовые, организационно-технические и др.). Вместе с тем факт наличия значительного количества киберправонарушений свидетельствует о необходимости разработки и использовании на практике новых эффективных способов борьбы с данными правонарушениями.

Считаем целесообразным, наряду с уже используемыми методами обеспечения кибербезопасности, применение следующих:

1. Включение в образовательный процесс учащихся школ и средних специальных учебных заведений, а также учреждений высшего образо-

вания учебных дисциплин (спецкурсов), направленных на изучение основ кибербезопасности. Полагаем, что в данном случае возможно использовать элементы таких учебных дисциплин, как «Основы права» и «Информационное право» и на их базе создать предмет «Основы информационного права» либо «Основы кибербезопасности». Это позволит в значительной степени снизить подверженность потенциальных жертв преступлениям в киберсфере. Думаем, что такая работа должна быть направлена в первую очередь на перечисленные выше категории населения, поскольку именно они наиболее простые потенциальные цели для киберпреступников и менее всего обладают информацией о возможных путях противодействия последним. Считаем целесообразным также введение форм контроля (например, зачет) по указанным спецкурсам для контроля за уровнем усвоения указанного материала учащимися.

2. В качестве эффективного профилактического мероприятия, направленного на повышение уровня знаний в области информационной безопасности (иными словами, направленной на повышение цифровой грамотности), будут выступать курсы повышения квалификации и курсы повышения мастерства по дисциплинам, указанным выше. Данные курсы, полагаем, необходимо проводить для сотрудников различных предприятий и организаций, а также сотрудников государственных органов на постоянной систематической основе, не реже чем один раз в 1–2 года, поскольку информация в этой сфере обновляется с достаточно высокой скоростью. Период обучения на таких курсах считаем целесообразным делать от 1,5 до 3 недель с последующей сдачей квалифицированного зачета либо защитой выпускных работ.

3. Очевидным и необходимым нововведением для Республики Беларусь может стать также разработка и использование комплекса компьютерных программ, которые будут способны заменить зарубежные аналоги, а также, с другой стороны, позволят государственным органам осуществлять значительно проще контроль за сферой кибербезопасности в стране.

В качестве наиболее эффективного метода поддержания необходимого уровня кибербезопасности на территории Республики Беларусь может стать открытие учебной дисциплины «Информационное право» на юридических факультетах крупнейших учреждений высшего образования страны. Это позволит подготовить необходимое и вместе с тем достаточное количество обученных специалистов, владеющих навыками и знаниями на высоком профессиональном уровне, а в дальнейшем с их помощью обеспечивать кибербезопасность Республики Беларусь.

Сфера кибербезопасности, цифровой грамотности и иные сферы, тесно связанные с информацией и информационными услугами, постоянно сталкиваются с новыми проблемами и угрозами, соответственно,

для их решения необходимы формирование и применение в практической деятельности новых способов (методов).

Кроме того, для более эффективного урегулирования области отношений, связанных напрямую со сферой кибербезопасности, необходимы, с нашей точки зрения, разработка и принятие комплекса нормативных правовых актов. В качестве значимого и центрального звена может выступить единый кодифицированный акт в информационной сфере – Информационный кодекс. Его подготовка, по нашему мнению, позволит урегулировать значительное количество правоотношений.

На основании вышеизложенного можно сделать следующие выводы:

1. Информация в целом и обеспечение кибербезопасности является важными элементами информационного общества и для его формирования и развития необходим комплекс эффективных мер, способных обеспечивать регулирование и защиту с различных направлений (правового, организационно-технического и др.).

2. Для обеспечения кибербезопасности необходим комплексный системный подход, который сможет обеспечить нахождение требуемых решений актуальных вопросов в данной сфере. В качестве основы применения такого подхода может стать создание учебной дисциплины «Информационное право» в крупнейших учреждениях образования Республики Беларусь.

3. Для обеспечения высокого уровня защиты кибербезопасности необходимо разработать и принять ряд нормативных правовых актов, направленных на поддержание данного уровня. В качестве центрального звена требуемых правовых актов может выступить единый кодифицированный правовой акт – Информационный кодекс.