БЕЗОПАСНОСТЬ КАК ЗАЛОГ УСПЕХА

Одной из главных забот руководителя финансово-кредитного учреждения или его отделения является стабильная работа возглавляемого им коллектива, функционирование всех служб и подразделений банка в соответствии с установленным регламентом. Любое отклонение от этого регламента приводит к сбоям в работе, а следовательно и к убыткам.

ИТОГИ

До недавнего времени к числу наиболее распространенных причин нарушения стабильной деятельности фирм и предприятий относили стихийные бедствия, пожары и хищение материальных ценностей, но с появлением новых форм собственности и рыночных отношений, с развитием новых информационных технологий все чаще приходится сталкиваться с проявлениями несанкционированного доступа к информации, терроризма и другими преступлениями, направленными на незаконное овладение корпоративной информации. Таким образом, одним из главных условий бесперебойной работы финансово-кредитного учреждения становится обеспечение безопасности его деятельности, что приобретает в сегодняшних украинских условиях все более сложный, разносторонний, комплексный характер и требует определенных материальных затрат. Эти затраты окупаются, если принятые меры сокращают или предотвращают ущерб от вышеуказанных угроз, а следовательно можно говорить об эффективных расходах на обеспечение безопасности. Впрочем, далеко не всегда затраты на безопасность повышают стабильность деятельности фирм и предприятий. Наиболее важные вопросы технической, физической и информационной безопасности банков и компаний, занятых в банковской сфере, были рассмотрены на IV Международной конференции «Безопасность финансово-кредитных учреждений: новые вызовы – новые решения – 2015», организованной специализированным журналом «Банкиръ».

IV МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

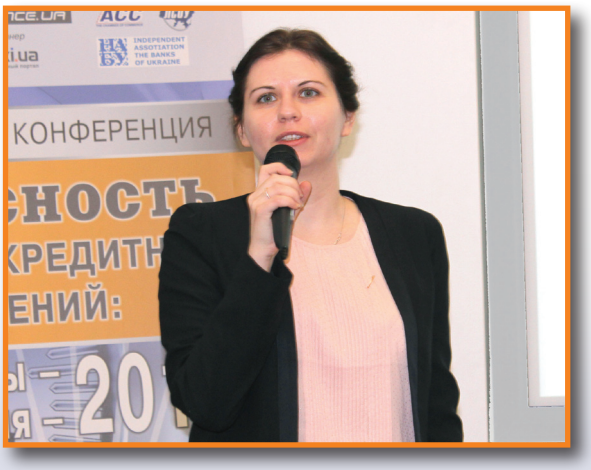
БЕЗОПАСНОСТЬ ФИНАНСОВО-КРЕДИТНЫХ УЧРЕЖДЕНИЙ:

новые вызовы – новые решения – 2015

Работа IV Международной конференции «Безопасность финансово-кредитных учреждений: новые вызовы – новые решения – 2015» была рассчитана на два дня и разделена на три тематических блока: «Законодательное регулирование в сфере безопасности деятельности финансово-кредитных учреждений в Украине. Международный опыт», «Информационная безопасность и борьба с мошенничеством. Техническая и физическая безопасность» и «Юридическое сопровождение деятельности финансово-кредитных учреждений. Работа с проблемными активами».

Жанна ГОЛИК
генеральный директор издательства «КБС-Издат», журнала «Банкиръ»

Работу конференции открыла *генеральный директор издательства «КБС-Издат», журнала «Банкиръ»* ***Жанна ГОЛИК***. Прежде всего, я хочу поблагодарить нашего генерального партнера, любезно предоставившего помещение для проведения конференции, – компанию «Майкрософт Украина», информационных партнеров – Американскую торговую палату в Украине, Лигу страховых организаций Украины и Независимую ассоциацию банков Украины. Медиа-партнерами нашего мероприятия выступают информационные порталы «Банки юэй», «Файнэнс юэй» и компания «Лаборатория Касперского». Также я благодарю всех участников и докладчиков конференции за то, что подготовили хорошие выступления, доклады и нашли время, чтобы присутствовать на нашем мероприятии. Журнал «Банкиръ» уже четыре года регулярно организовывает международные конференции, и на этом мероприятии учасникам предоставлена возможность обсудить насущные вопросы, пути развития, эффективные практические подходы, способствующие дальнейшему развитию банковского дела. Кроме того, мы четко отслеживаем ситуацию на рынке кредитно-финансовых услуг и организовываем подобные встречи, исходя из новейших тенденций, и в этот раз подготовили все условия для успешного заимствования международного опыта работы.



Элизабет СОЛОВЬЕВ
торговый атташе посольства Государства Израиль в Украине

Украину часто сравнивают с Израилем. У наших стран действительно есть много общего. Украина, на мой взгляд, имеет колоссальный потенциал для развития, однако, чтобы страна развивалась, важна готовность государства создавать позитивный инвестиционный климат и вкладывать собственные средства в развитие инфраструктуры. Пример Израиля в данном случае красноречив: каждый доллар, вложенный государством в экономику страны, принес семь долларов прибыли. Также важным фактором развития страны явилась кооперация между индустрией и университетским образованием. Удачным примером такой синергии являются созданные технологии капельного орошения, инновационные медицинские технологии (компьютерные томографические и ультразвуковые сканеры, хирургические лазеры), технологии очистки воды, переработки бытовых отходов, солнечная энергетика, и, конечно, технологии в сфере кибербезопасности. Торгово-экономический отдел Посольства Государства Израиль способствует развитию и взаимовыгодному укреплению билатеральных связей наших стран. Мы видим серьезный потенциал развития сектора банковской безопасности в Украине и надеемся на плодотворное сотрудничество в данной сфере.

Алексей СИРАКОВ
координатор Комитета по вопросам банковской инфраструктуры и платежных систем Независимой ассоциации банков Украины

С приветственным словом от имени Независимой ассоциации банков Украины выступил координатор Комитета по вопросам банковской инфраструктуры и платежных систем НАБУ ***Алексей СИРАКОВ***, который отметил увеличившийся интерес украинских банков к поискам новых решений, позволяющих защитить не только предоставляемые услуги, но и оптимизировать расходы на их внедрение, и от имени Ассоциации выразил признательность и благодарность организаторам за проведение мероприятия.

Люк ЯКОБЗ
Чрезвычайный и Полномочный Посол Королевства Бельгия в Украине

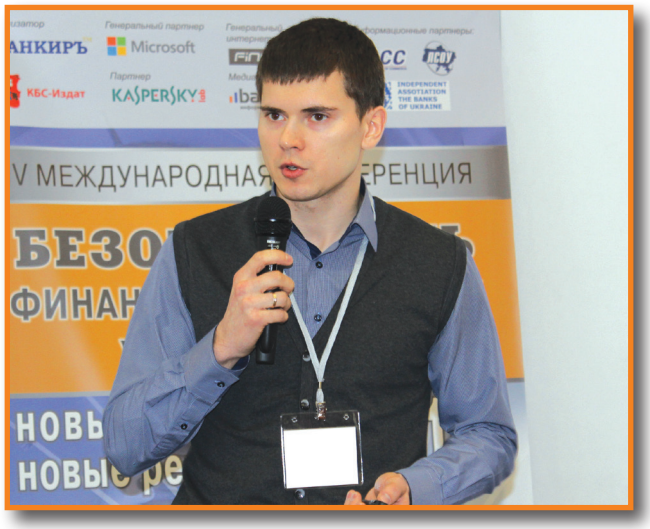
Бельгийская банковская система представляет собой многообразие финансово-банковских и кредитных учреждений, которые работают в различных секторах рынка. Бельгийский банковский ландшафт весьма интернационален: из 104 банков, действующих в Бельгии, 89 принадлежат иностранным группам, а 15 – банки с бельгийским капиталом. Экономика развивается параллельно с обществом, равно как и банковский сектор следует по тропе экономической эволюции. Некоторые изменения вполне очевидны. Во-первых, общество становится все более «цифровым» – клиенты банков все чаще прибегают к использованию мобильных устройств и цифровых технологий. Во-вторых, их требования постоянно совершенствуются и становятся все более изощренными. В-третьих, важную роль играет уверенность клиента в избранном банке. Что касается безопасности, то следует отметить, что за последние 10-15 лет значительно снизилось количество банковских ограблений, в основном благодаря активной политике в сфере ограничения доступа к наличным средствам в сети банковских отделений. В то же время увеличилось количество пользователей интернет- и мобильного банкинга, в связи с чем возросло количество случаев интернет-мошенничества. Впрочем, бельгийские банки постоянно инвестируют в развитие эффективных решений в сфере обеспечения безопасности системы и кампании по повышению осведомленности пользователей банковских услуг, и это, разумеется, значительно сокращает возможности мошенников.

Юрий КОЗЛОВ
начальник отдела по организации предоставления услуг ЭЦП и сопровождения ИТС ЦУО государственного предприятия «Информационный центр» Министерства юстиции Украины

Внедрение современных средств и схем электронной идентификации в Украине с высоким уровнем гарантий идентификации и аутентификации открывает возможности для граждан Украины на новом качественном уровне осуществлять взаимодействие с государственными и местными органами власти, получать электронные административные услуги.

Такое внедрение представляет собой одну из основных задач для правительства Украины по модернизации систем электронного управления. Выбранный государством курс на евроинтеграцию однозначно предусматривает стремление к соответствию нормативным актам, стандартам и процедурам, принятым в странах Европейского Союза, единым для всех государств-членов.

Поэтому разработка и запуск современных средств и схем электронной идентификации требует детального анализа различных аспектов состояния и трендов этой сферы как в Украине, так и в государствах-членах Европейского Союза.



Николай КОВАЛЬ
Государственная служба финансового мониторинга Украины

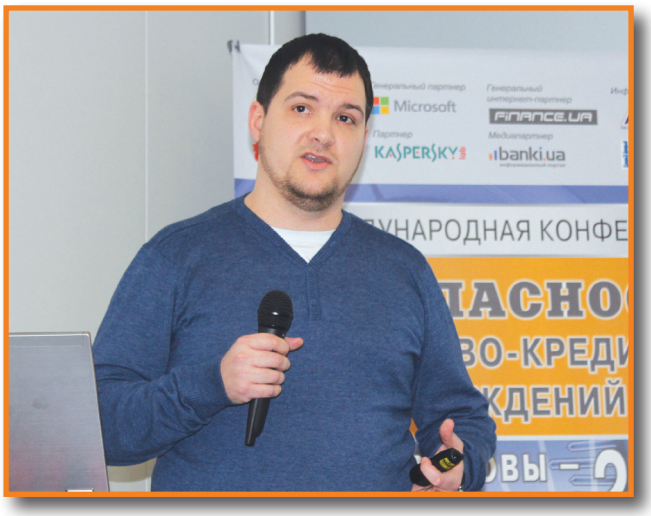
Во время своего доклада на тему «Небумажной безопасность» Николай Коваль из Команды реагирования на компьютерные чрезвычайные события Украины «CERT-UA», функционирующей на базе Государственной службе специальной связи и защиты информации Украины, осветил основные результаты работы «CERT-UA» за последний год. Были приведены примеры разоблачения бот-сетей и эффективной отработки скомпрометированных данных, осуществляемой при координации «EMA», с разными украинскими банками. Денежный эквивалент потенциально предотвращенных финансовых потерь составил более 50 млн грн. Кроме этого, был произведен краткий экскурс по разработанным специалистами «CERT-UA» системам, в частности: IP Guard FEEDs и IP Guard AMS 1.0, а также продемонстрирован пример борьбы с нашумевшим мобильным ботнетом «Привет :) тебе фото», который атаковал более 100 тыс. смартфонов украинцев.

Бартош ФУРМАН
эксперт Отдела содействия торговли и инвестициям Посольства Республики Польша в Украине

Банківська система Польщі складається з трьох основних елементів – банків (Центральний банк, кооперативні та комерційні банки), системи взаємозв'язків між ними та їхнім оточенням і правової інфраструктури, що регулює діяльність зазначених інституцій, – і виконує низку функцій: емісійну і регулятивну, депозитно-кредитну, розрахункову, стимулятивну, розподіл ресурсів, фінансовий консалтинг. Основною метою Національного банку Польщі є збереження стабільності цін за сприянням економічної політики уряду доти, доки це не обмежує основну мету НБП. Фінансова інспекція, яка прийняла на себе обов'язки Комісії з банківського нагляду на 1 січня 2008 року, здійснює нагляд за діяльністю всіх банків у Польщі. Нагляд за діяльністю Комісії здійснює прем'єр-міністр. Обов'язки фінансової інспекції – банківський нагляд, пенсійний нагляд, страховий нагляд. Станом на 1 січня 2014 року польський банк PKO Bank Polski посідає 8 місце серед найбільших банків Центральної та Східної Європи, маючи 55,5 млрд євро активів і володіючи 2,2% польського банківського сектору.

Юрий КОГУТ
генеральный директор ООО «Консалтинговая компания «СИДКОН»

Банковские организации сегодня все чаще сталкиваются с таким широким спектром существующих угроз, как компьютерное мошенничество, компьютерные вирусы, взлом компьютерных систем, отказ в обслуживании и т. д. Высокая зависимость банковских организаций от информационных ресурсов, объединение корпоративных сетей и сетей общего доступа, совместное использование информационных ресурсов повышают уязвимость организаций от подобных угроз. Сегодня для банков жизненно необходима комплексная система информационной безопасности, которая задействует не только технические, но и организационные ресурсы. Создание комплексной системы информационной безопасности может обойтись для банка значительно дешевле, чем ликвидация последствий угроз ИБ. Для разработки системы ИБ банка необходимо отнести информацию к категории продукта ограниченного доступа; прогнозировать и выявлять угрозы безопасности информационным ресурсам; создать условия функционирования с наименьшей вероятностью реализации таких угроз и нанесения различных видов ущерба.



Олег ДУБИНА
Группа информационной безопасности «ФС Груп»

«Форум» – это виртуальная площадка, общения носителей и искателей специфических знаний, которые в той или иной мере относятся к хакерской среде. Разведка на хакерских форумах – это сбор, анализ и использование информации об участниках форумов, проводимые для предотвращения и расследования киберпреступлений, а также идентификации лиц, причастных к их совершению. «Forum Intelligence», является частным случаем OSINT и «Competitive Intelligence» применяемых в сфере исследований инцидентов компьютерной безопасности и раскрытия киберпреступлений. Хакерский форум – это виртуальная площадка, на которой происходит общение лиц, относящих себя к хакерской субкультуре, имеющих специальные знания в сфере компьютерных технологий и использующих их на практике. Среда хакеров, как любая другая субкультура наравне со своим языком (сленгом), базовыми идеалами и принципами, имеет и свою среду общения.

Ярослав БОЦМАН
главный консультант отдела разработки системных решений «ЭС ЭНД ТИ УКРАИНА»

В настоящий момент большинство атак на системы дистанционного обслуживания банковских клиентов осуществляется с помощью браузера. Вредоносное программное обеспечение предназначено для сбора и отправки конфиденциальных данных, используемых пользователями для осуществления финансовых транзакций. Одним из наиболее распространенных методов получения информации является отслеживание нажатий клавиш и создания снимков экрана, а также встраивание троянских модулей в операционную систему и браузер жертвы. Вредоносное программное обеспечение маскирует свои действия, осложняя поиск и борьбу антивирусам и специализированным антишпионским приложениям. Вред от этих типов атак не ограничивается потерей финансовых средств обманутых пользователей. Для финансового учреждения они также включают непрямые потери на проведение расследований и анализ транзакций, дополнительные затраты на обслуживание клиентов (увеличение нагрузки на контакт-центр и специалистов операционного зала) и перевыпуск карточек, а также оплату штрафов и затраты, вызванные потерей бизнес-репутации.

Михаил НЕЩЕРЕТ
ведущий специалист компании «DATAS Technology»

Решение Trustifier KSE (Kernel Security Enforcer) защищает информацию и противодействует утечке конфиденциальных данных с рабочих мест сотрудников и серверов компании. Это программное обеспечение информационной безопасности, которое защищает информацию и гарантирует, что конфиденциальные данные не могут выйти за определенные границы, независимо от того, кто имеет доступ к системе (в т.ч. администратор). Пользователи не видят информацию, которую не должны, они не могут собрать воедино кусочки информации, чтобы получить больше знаний, чем должны, они не могут использовать данные не по прямому назначению и имеют ограниченный доступ. KSE имеет несколько дополнительных уровней безопасности, которые позволяют предотвратить кибер-шпионаж.

Дмитрий ПОПОВ
менеджер по корпоративным продажам компании «Kaspersky Lab»

Существуют два наиболее распространенных сценария проникновения в Сеть: фишинговая рассылка, когда на почтовый ящик клиента приходит письмо с зараженной ссылкой, которую клиент очень часто из-за непонимания размеров угрозы открывает. Второй сценарий – заражение через соцсети, когда злоумышленники умело набиваются вам в друзья, реагируют на ваши записи, общаются с вами как обычные пользователи, ставят лайки, делают все, чтобы втереться к вам в доверие и спустя какое-то время таки отправляют вам под самым безобидным предлогом фишинговую ссылку, через которую уже и происходит заражение устройства или приложения. Защитные продукты компании *«Kaspersky Lab»* ориентированы не только на решение существующих проблем, но и на предотвращение новых, еще неизвестных угроз. Решения компании обеспечивают многоуровневую систему безопасности электронных платежей, вне зависимости от типа используемого устройства, при этом эффективно используя ресурсы виртуальной инфраструктуры и не оказывая существенного воздействия на ее производительность, соответствуют всем основным требованиям, включая высочайший уровень защиты, адаптируемость к меняющимся условиям, совместимость с различными платформами, отказоустойчивость и т.д.

Андрей САБЛИН
директор Центра сертификации банковского оборудования, сооружений безопасности, средств защиты и систем качества

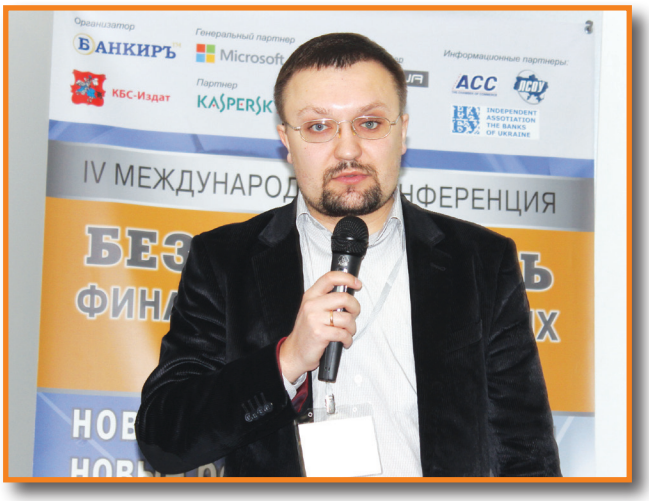
В своем докладе «Пуле- и взломостойкие конструкции» отметил, что на сегодняшний момент службы безопасности банков не владеют в совершенстве теоретической базой знаний и стандартов, касающихся технической и физической безопасности финансово-кредитных учреждений. Например, они не осознают разницы между пулестойкими, ударопрочными и взломостойкими конструкциями. Андрей Саблин также осветил нормы ряда также украинских стандартов, как ДСТУ EN 356:2005 «Скло в будівництві. Захисне скління. Випробування та класифікація за тривкістю щодо ручного зламування», ДСТУ ENV 1627 «Окна, двери и жалюзи. Сопротивление взлому. Классификация и технические требования», ДСТУ 4546:2006 «Захисне скління», ДСТУ 4547:2006 «Окна, двери и жалюзи. Пулестойкость. Требования и классификация».

Игорь ГУСКА
заместитель начальника управления – начальник отдела Департамента информационной безопасности Национального банка Украины

Сегодня банки заинтересованы в предоставлении клиенту максимального объема услуг надлежащего качества с высоким уровнем безопасности без посещения офиса банка. В связи с этим возникает ряд вопросов, касающихся безопасности систем дистанционного банковского обслуживания, как то: защищенный обмен между клиентом и банком, обеспечение доверенной среды как на клиентском рабочем месте, так и в банковской части системы ДБО. Кроме того, важными факторами становятся возможность дистанционного открытия счета и получение юридически значимого электронного платежного документа в рамках системы дистанционного обслуживания.

Наталия ЛЕСИК
сотрудник рабочего аппарата украинского бюро ИНТЕРПОЛа

Современные тенденции преступности, выход за пределы государств, абсолютный и относительный рост, особенно ее организованных форм, транснациональный, а во многих случаях и глобальный характер, обусловили объединение усилий государств путем международного сотрудничества в борьбе с преступностью. Особая роль в таком сотрудничестве ныне принадлежит международным правоохранительным организациям. Они представляют собой объединения суверенных государств межправительственного характера, учрежденные межгосударственными договорами, созданные на основе межгосударственных соглашений (устава или иного учредительного документа), имеющие постоянные органы, наделенные международной правосубъектностью, и осуществляющие с соблюдением общепризнанных принципов и норм международного права деятельность по обеспечению правовой защиты личности, общества, государств и мирового сообщества от международных преступлений, преступлений международного характера, а также транснациональных преступлений, посягающих на внутригосударственный правопорядок, борьбу с такими преступлениями. Одним из старейших таких объединений является Международная организация уголовной полиции – Интерпол.



Алексей НАЙДА
директор по развитию бизнеса компании «Efficient IT»

Тема идентификации и аутентификации сегодня актуальна и интересна. Для идентификации лиц существует ряд привычных инструментов, которыми мы можем оперировать, тогда как в мире информационных технологи идентификатор человека – это некая запись в базе данных. И с этим моментом сопряжен ряд проблем. В нашей работе мы ориентируемся на решения компании «Gemalto». Это успешная европейская компания, работающая в сфере электронной безопасности. Только за 2013 год ею было подано и зарегистрировано более 100 патентов в области информационной безопасности. Специалисты компании разрабатывают ряд направлений, которые могут быть актуальны не только для бизнеса. Компания считается одним из лидеров по производству сим-карт мобильных телефонов. Также постоянно ведутся разработки решений для управления безопасностью данных с акцентом на клиентуру из банковского сектора. За 2012 год компания продала более 2 млрд аппаратных компонентов и решений в области информационной безопасности.

Шаи ВАРДИ
вице-президент компании «SuperCom», руководитель отдела финансовых решений

Компания «SuperCom» является лидером рынка информационных технологий в сфере электронной радиочастотной идентификации и в настоящий момент владеет 7-ю патентами. Мы сотрудничаем более с чем 20 странами мира и зарегистрированы на бирже «Nasdaq» с 2005 года. Наша компания предлагает программный пакет «SuperPay» для безопасных мобильных платежей. «SuperWallet» (преобразует любое мобильное устройство в безопасный кошелек для платежей), «SuperTAP» (позволяет осуществлять мобильные платежи с помощью любого мобильного устройства), «SuperPOS» (конвертирует мобильное устройство в терминал для приема платежных карт) и «SafeMoney» (защита и предотвращение угроз и атак на мобильное устройство).

Александр ЗАЛЕТОВ
член Национальной комиссии, которая осуществляет государственное регулирование в сфере рынков финансовых услуг

Основними векторами реформування ринків небанківських послуг України, зокрема страхового ринку, є:

1. Усунення надмірного регулювання, оптимізація реєстраційних та дозвільних процедур, вдосконалення регуляторних норм та правил як засобу адекватного реагування на сучасні економічні виклики, гармонізація вимог згідно з Директивами ЄС;
2. Перехід від тотального контролю до автоматизованого дистанційного пруденційного нагляду на основі впровадження необтяжливих та ефективних наглядових процедур, вдосконалення системного аналізу та дистанційного моніторингу;
3. Відновлення довіри споживачів страхових послуг та інвесторів за рахунок підвищення вимог до забезпечення прозорості страхового ринку, створення дієвої системи захисту їх законних прав, формування надійних механізмів убезпечення коштів інвесторів та громадян;
4. Запровадження цільових показників розвитку страхового ринку та KPI регулятора.

Лилия ОЛЕКСЮК
председатель Всеукраинской ассоциации «Информационная безопасность и информационные технологии»

ВАЙБИТ создана для удовлетворения и защиты интересов лиц, намеревающихся развивать сектор информационной безопасности, информационных технологий и занятых в сфере защиты персональных данных в Украине. Из основных задач Ассоциации – сотрудничество с органами государственной власти, общественными и профессиональными союзами, участие в формировании, развитии и реализации политики государства в означенных сферах, а также в сфере криптографической и технической защиты информации.

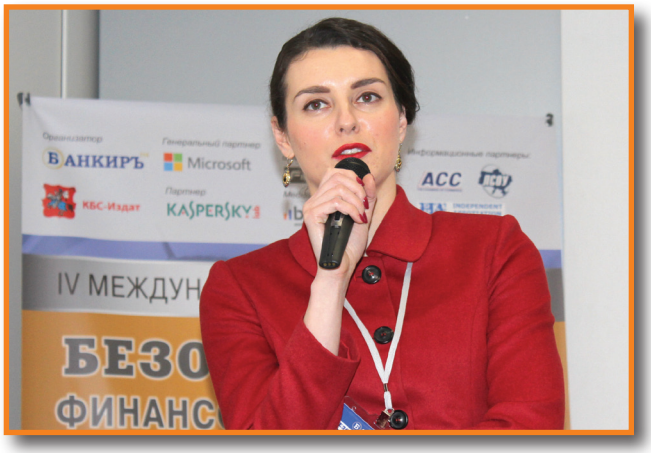
В докладе было обращено особое внимание на оформление отношений банка с клиентами с учетом законодательства в сфере защиты персональных данных, а именно – необходимость учитывать в договорах передачу информации о заемщике третьим лицам с целью взыскания задолженности. Родственники должника не являются участниками кредитных отношений с банком (кроме случаев поручительства), соответственно передача данных о них третьим лицам может быть расценена как безосновательное противоправное вмешательство в личную жизнь и нарушением их конституционных прав.

Наталья БУРЛАКОВА
руководитель группы серверных решений компании «Microsoft»

Технологические угрозы становятся все быстрее, изощреннее и все более ориентированными на извлечение выгоды. Предприятиям необходимо иметь возможность оценить общее состояние безопасности своей инфраструктуры, без лишних усилий внедрить и верно настроить средства защиты от известных и будущих угроз, а также быстро выявлять и локализовывать любые атаки и устранять их последствия. Одновременно с этим требуются и средства для эффективного и безопасного мониторинга, контроля и создания отчетов по доступу к корпоративной информации и ресурсам. Учет должен вестись в отношении сотрудников, партнеров и клиентов, получающих доступ к широкому спектру приложений с любого устройства и из любого месторасположения. Для выполнения всех этих задач корпорация «Майкрософт» считает необходимой разработку комплексного набора решений по обеспечению информационной безопасности и контроля доступа. Эти средства позволят отделу IT справляться с постоянно меняющимся фронтом угроз, а предприятие сможет продолжать свою работу на максимальном уровне производительности и эффективности.

Ирина ИВЧЕНКО
директор по аудиту, консалтингу и сертификации ООО «Центр Системных Интеграций (SICenter)»

Компания «Центр системных интеграций» уже несколько лет оказывает помощь банкам Украины по вопросам внедрения и сопровождения системы управления информационной безопасностью. Вопросам информационной безопасности и кибербезопасности в мире уделяется огромное внимание – приняты новые международные стандарты. В настоящий момент Украина вовлечена в обширную информационную войну, прямо отражающуюся на всех сферах жизни общества. Анализ международных стандартов по вопросам обеспечения кибербезопасности показал, что внедрение системы управления информационной безопасностью в значительной мере соответствует требованиям обеспечения кибербезопасности. Следует отметить, что в Украине еще не разработана законодательная база, которая регулирует вопросы кибербезопасности. Поэтому выполнение требований и процедур системы управления информационной безопасностью, тщательная оценка рисков, связанных с использованием информационных технологий, обеспечивает защиту банков в том числе и от кибератак.



Марина САЕНКО
адвокат, партнер юридической компании «Закон Победы»

Современные реалии диктуют новые правила игры на рынке банковских услуг, расширяя сферы угроз банковской безопасности. Как показывает наш опыт, построению эффективной системы безопасности банка способствует ее анализ через призму объектов посягательств (денежные активы, недвижимость, информационные ресурсы, клиентская база, репутация) и потенциальных субъектов угроз. В последнее время наибольший ущерб банкам причиняется его собственниками и топ-менеджментом банков, а также сотрудниками, в том числе с использованием методов конкурентной разведки. Кроме того, негативно влияют на процессы прогнозирования и выстраивания системы банковской безопасности постоянно изменяющаяся законодательная база, нестабильная экономическая ситуация и коррупционная составляющая.

Алексей КРАСЮК
заместитель директора по операционным вопросам и информационной безопасности в «ЕМА»

Очень важно понимать, что сегодня мошенники «мигрируют» из одного вида мошенничества в другой. Это подтверждают многочисленные факты в рамках межбанковского обмена в системе «Exchange-Online». Для мошенников нет физических границ, они их легко пересекают, равно как нет границ и для информации – главного орудия в руках мошенников. Для эффективного противодействия и нам необходимо активно обмениваться информацией о случаях мошенничества. Основными критериями в этом взаимообмене является актуальность информации и количество его участников. Ассоциация «ЕМА» объединяет 117 банков и платежных агрегаторов из Украины, Молдовы, Белоруссии, Росии и Казахстана, поддерживает партнерские связи с зарубежными организациями и ведет двусторонний обмен данными об АТМ-мошенничестве с 35 странами мира. Обмен помогает отслеживать тренды мошенничества в других странах и делать прогнозы их появления в Украине.

Дмитрий СТРИЖОВ
генеральный директор холдинга охранных предприятий «Шериф»

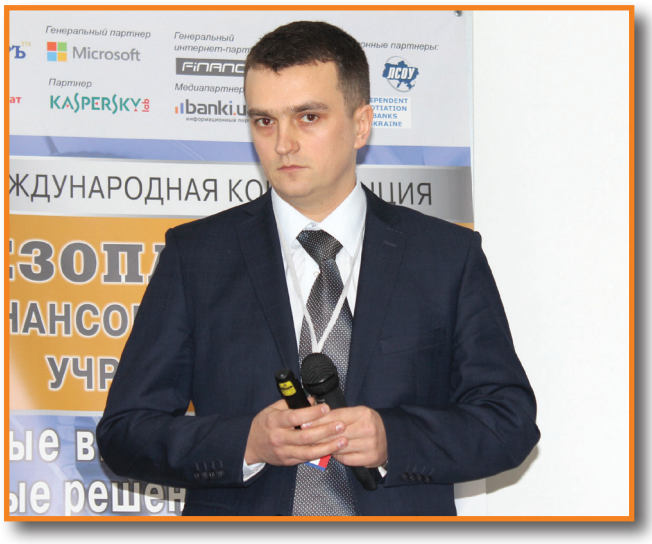
На протяжении 12 лет охранная компания «Шериф» следует избранному девизу – «Защищать и охранять». За эти годы «Шериф» в разных кругах стал синонимом качественных и надежных охранных услуг. В 2014 году «Шериф» стал лучшим охранным предприятием Украины в соотношении цена-качество. Внедрена программа «Абсолютная защита», которая предоставляет уникальную возможность получить весь спектр услуг охраны и безопасности из одних рук: охранной и тревожной сигнализации; сопровождение инкассаторов, денежных средств и грузов; проектирование, установка, обслуживание и наблюдение пожарной сигнализации; услуги по измерению сопротивления изоляции; услуги по физической охране объектов, организации контрольно-пропускного режима; охрана массовых мероприятий; установка систем видео-наблюдения и контроля доступа. Нашей организации доверяют свою безопасность посольства европейских государств, коммерческие предприятия, особо важные государственные предприятия.

Алексей АТРОЩЕНКО
председатель правления Ассоциации «Украинский центр развития внебиржевых финансовых инструментов и технологий»

Политический и экономический кризис, когда финансовая система пребывает в не лучшем состоянии, вкладчики забирают свои депозиты, а должники не возвращают кредиты, создает наиболее благоприятные условия для появления финансовых пирамид. За последние 10 лет на территории постсоветского пространства было зарегистрировано более 35 млн лиц, пострадавших от подобных структур. Финансовые пирамиды совершенствуются, маскируются, придумываются новые методы привлечения клиентов. Среди наиболее существенных причин появления и функционирования финансовых пирамид – низкий уровень финансовой грамотности населения, желание людей быстро разбогатеть без приложения особых усилий. Усложняет проблему отсутствие в Украине правовых механизмов борьбы с финансовыми пирамидами. Мошенники это осознают и активно этим пользуются. Ассоциация УЦРФИН призывает участников финансового рынка, регуляторов и экспертов объединить свои усилия для принятия законодательства, ограничивающего возможности создания и функционирования финансовых пирамид.

Галина ТРЕТЬЯКОВА
генеральный директор Ассоциации «Украинская федерация страхования»

Структура регулирования, внедренная в Украине, существует в некоем постоянном конфликте, причины которого проистекают из прямого нарушения конституционных норм. Оно заключается в том, что, согласно Конституции Украины регуляторы рынка, кроме председателя Национального банка Украины и Антимонопольного комитета Украины, имеют право назначать только Кабинет Министров или Премьер-министр, тогда как по факту это делает Президент. Следовательно, именно он несет ответственность за осуществление регулятором его полномочий. За двадцать с лишним лет независимости руководство государства Украина так и не сумело последовательно и на равных условиях распределить эти полномочия, и теперь мы столкнулись с ситуацией, когда все рынки сконцентрированы в одном регуляторе: лизинг и страховой рынок, факторинг и бюро кредитных историй, негосударственные пенсионные фонды и ипотечные учреждения и т.д. Словом, огромное количество секторов надзирается одним регулятором и, когда речь заходит о его реорганизации, логично, что дальше этого дело не идет, потому что разобраться в том, кто за что отвечает, практически невозможно.



Василий ГУЗИЙ
начальник отдела борьбы с преступлениями в сфере платежных систем Управления по борьбе с киберпреступностью Министерства внутренних дел Украины

Протягом 2014 року управління боротьби з кіберзлочинністю провело 3-и міжнародних розслідування з документування злочинних груп, причетних до легалізації коштів, одержаних від кіберзлочинності. У Федеративній Республіці Німеччина – розслідування на предмет відмивання грошей, одержаних від функціонування шкідливого програмного забезпечення «Ransonware» (вірус, що блокує операційну систему). У Республіці Австрія, Королівстві Бельгія та Великій Британії – щодо відмивання грошей, одержаних від банківських троянів «Spyeye», «Zeus», «Torpig». У Сполучених Штатах Америки – щодо відмивання грошей, одержаних у результаті функціонування шкідливого програмного забезпечення «Shylock». Також у минулому році нами опрацьовано 15 міжнародних запитів стосовно легалізації коштів, викрадених із рахунків іноземних банків на території України. Недосконалість законодавчої бази, відсутність досвіду документування, брак судової практики, відсутність належної взаємодії між слідчими, оперативними підрозділами та органами прокуратури і недостатня міжнародна співпраця значно перешкоджають розслідуванню і водночас сприяють поширенню злочинів у сфері ІБ.

Вячеслав ЗАРИЦКИЙ
ведущий технический специалист компании «ESET»

Более 25 лет компания ESET предоставляет качественную IT-защиту корпоративной сети. Построенные на основе уникальной технологии ThreatSense®, облачных и других современных технологиях, решения ESET обеспечивают эффективную защиту от всех известных и ранее неизвестных, а также скрытых угроз. Флагманским продуктом компании является комплексное решение ESET Endpoint Security. В отличие от классической антивирусной программы данное решение обладает дополнительными модулями и обеспечивает защиту не только от различных вредоносных программ, но и от многих других распространенных видов интернет-угроз, атак хакеров, надоедливого спама, кражи конфиденциальных данных, посещения вредоносных и поддельных веб-ресурсов, использования несанкционированных медиа-носителей и многих других угроз. В продуктовую линейку ESET входят решения для защиты файловых и почтовых серверов, интернет-шлюзов, продукты для защиты мобильных и портативных устройств, решения для аутентификации и шифрования данных, а также пакеты программ, объединяющие в себе перечисленные программы и позволяющие оптимизировать затраты на решения безопасности.

Алексей ГРЕБЕНЮК
директор ИТЦ «ХАЙ-ТЕК БЮРО»

Банковский сектор приковывает все больше внимания компьютерных злоумышленников всего мира. Махинации с банковскими картами происходят повсеместно. Раньше наиболее актуальными проблемами службы безопасности были предотвращение физического взлома банкомата и установки поддельных устройств поверх лицевых панелей банкомата, борьба с хищением банковских карт и выдаваемых денег. Участившиеся случаи кибернетического скимминга на территории СНГ, а также все более изощренные методы атак – это факты, свидетельствующие о том, что банки и обслуживающие компании должны совершенствовать меры безопасности и следить за последними новостями индустрии и лучшими мировыми практиками. В рамках расследований наша компания анализирует значительное количество нарушений, связанных с утечками данными платежных карт и рассматривает большое количество вредоносных программ, которые направлены на POS-терминалы. Вредоносные программы для POS предназначены для кражи данных трека (критичные данные, хранящиеся на магнитной полосе платежной карты), либо из памяти или физического диска машины.

Эффективность системы комплексной защиты банка может быть обеспечена путем рационального сочетания множества функций, средств и методов. Они должны объединяться в единый, целостный механизм защиты, создание которого лучше всего вести параллельно с проектированием и возведением финансово-кредитного объекта. Функционирование системы комплексной защиты должно планироваться и обеспечиваться, в том числе и финансами, наряду с планированием и обеспечением жизнедеятельности всего банка. Важнейшим обстоятельством, способствующим обеспечению безопасности, является личная заинтересованность персонала в надежном функционировании защиты. Разумная кадровая политика руководства, воспитывающая стремление к стабильности в сочетании с материальной заинтересованностью у всего персонала банка будет залогом эффективной работы системы комплексной защиты в качестве надежного барьера на пути нарушителей и злоумышленников.

Разумеется, темы, рассмотренные в ходе проведения IV Международной конференции «Безопасность финансово-кредитных учреждений: новые вызовы – новые решения – 2015», отнюдь не охватывают абсолютно весь спектр теоретических и практических вопросов безопасности финансово-кредитных учреждений. Однако организаторы мероприятия создали максимально комфортные условия для участников и гостей конференции и обеспечили высочайший уровень обмена знаниями и опытом ведущих международных компаний и специалистов, и это маленький шаг на пути Украины к работе по наивысшим стандартам.

Подготовил Егор ЕРШОВ

ПАНЕЛЬНАЯ ДИСКУССИЯ

«ОСОБЕННОСТИ ВНЕДРЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В УКРАИНЕ»

В последнее время в мире постоянно увеличивается количество проектов, целью которых является организация обмена конфиденциальной информацией в любой сфере деятельности, например, между предпринимателями и государственными органами. Сегодня все больше компаний в своей работе прибегают к «безбумажным», информационным технологиям передачи данных, в том числе и конфиденциальных.

Предпосылки для введения систем электронного документооборота создаются и активно продвигаются и в законодательном органе государства. Так, в Украине правовой статус безбумажного документооборота с применением электронной цифровой подписи определяется двумя законами, принятыми 22 мая 2003 года – «Об электронных документах и электронном документообороте» № 851-IV и «Об электронной цифровой подписи» № 852-IV. Вопросы применения положений указанных законов регламентируются постановлениями Кабинета Министров Украины от 28 октября 2004 года: «Об утверждении Порядка применения электронной цифровой подписи органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями государственной формы собственности» № 1452 и «Об утверждении Типового порядка осуществления электронного документооборота в органах исполнительной власти» № 1453. Впрочем, несмотря на довольно солидный пакет нормативно-правовых актов относительно обеспечения безбумажных процедур документооборота, главным пробелом остается отсутствие определенных норм относительно осуществления электронного делопроизводства.

Электронный оборот более эффективен за счет того, что он легче поддается оптимизации. Затраты на внедрение систем электронного документооборота окупаются не только за счет повышения скорости обмена информацией и сокращения расходов на хранение документов, но и отсутствием серьезных затрат на перестройку документооборота при возникшей необходимости. По данным ряда международных исследований, в развивающихся компаниях бумажный документооборот с каждым годом возрастает примерно на 15-25%, порядка 30% времени рабочих групп расходуется на поиски и согласование документов, 6% документов безвозвратно теряются, каждый внутренний документ копируется до 20 раз. В среднем каждый сотрудник тратит 150 часов в год на поиск утерянной информации, что в результате приводит к значительному снижению производительности труда персонала компаний.

Целью применения систем цифровой подписи является аутентификация информации – защита участников информационного обмена от навязывания ложной информации, установление факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений. Система цифровой подписи предполагает, что каждый пользователь сети

имеет свой секретный ключ, который используется для формирования подписи, а также соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи. Цифровая подпись вычисляется на основе секретного ключа отправителя информации и собственно информационных бит документа. Проверить подпись может любой пользователь, имеющий открытый ключ, в том числе независимый арбитр, который уполномочен решать возможные споры об авторстве сообщения (документа).

Одной из первых отраслей в Украине, в которой был внедрен электронный документооборот платежных документов, еще в 1994 году стал банковский сектор. Благодаря положительным результатам работы системы электронных платежей, в том числе и использования ЭЦП для подписания платежных электронных документов (с 1995 года), к использованию ЭЦП впоследствии начали приобщаться и компании других сфер деятельности. Однако, несмотря на неплохой «старт», в настоящий момент в этой сфере, к сожалению, больше вопросов, нежели ответов. Для решения некоторых проблем международный журнал «Банкиръ» 26 февраля 2015 года организовал панельную дискуссию – «Особенности внедрения электронной цифровой подписи в Украине», которая прошла в рамках IV Международной конференции «Безопасность финансово-кредитных учреждений: новые вызовы – новые решения – 2015».

Среди приглашенных гостей были участники и докладчики конференции, а спикерами в ней выступили: Юрий Козлов – начальник отдела по организации предоставления услуг ЭЦП и сопровождения ИТС ЦУО государственного предприятия «Информационный центр» Министерства юстиции Украины, Ирина Ивченко – вице-президент Киевского отделения «ISACA», Мария Горностай – советник в Администрации Президента Украины, а также Владимир Козак – заместитель председателя Государственной службы Украины по вопросам защиты персональных данных.

В ходе панельной дискуссии участники выделили такие основные тезисы.

Мария ГОРНОСТАЙ

советник,
Администрация
Президента Украины

Наразі практика застосування електронного цифрового підпису, що склалася в Україні, не відповідає світовій. Але ми поступово рухаємося в бік євроінтеграції, прагнемо застосовувати європейський досвід, а тому нам слід диференціювати випадки, коли потрібно застосовувати ЕЦП, зробити його зручним у застосуванні як для бізнесу, так і для громадського сектору. По-друге, у вирішенні багатьох питань, пов'язаних із застосуванням та впровадженням ЕЦП, Україні допоможе націоналізація світових стандартів. На мою думку, застосування електронного цифрового підпису в банківському секторі є взірцем того, як цей процес має виглядати в ідеалі (і водночас має свої відмінності) порівняно із застосуванням ЕЦП в інших сферах. Вони полягають як у форматі, так і в алгоритмах застосування.

Юрий КОЗЛОВ

начальник отдела по организации предоставления услуг ЭЦП и сопровождения ИТС ЦУО государственного предприятия «Информационный центр» Министерства юстиции Украины

На мой взгляд, один из тех вопросов, которые интересуют представителей банковского сектора в Украине, – нужна ли нам существующая дуальная модель инфраструктуры открытых ключей, нормативного и технического регулирования сферы ЭЦП?! Сейчас за регулирование сферы ЭЦП в системах электронного документооборота отвечает Министерство юстиции, в то время как за использование ЭЦП в банковской сфере отвечает Национальный банк Украины. В связи с этим в Украине фактически нет единой политики использования ЭЦП, что препятствует взаимному проникновению услуг цифровой подписи из одной сферы в другую. Возможно, на законодательном уровне следует рассмотреть вопрос о создании единого центра юридического и технологического тяготения в отношении регулирования сферы ЭЦП и уйти от двойных стандартов и, порой, несовместимых процедур. Сейчас, когда готовятся изменения в Закон Украины «Об электронной цифровой подписи», это сделать вполне реально.

заместитель председателя Государственной службы Украины по вопросам защиты персональных данны

Владимир КОЗАК

В ходе подготовки закона об ЭЦП 2003 года не были строго прописаны требования безопасности для средств создания ЭЦП, как это сделано в европейской директиве: данные, используемые для создания подписи, не могут извлекаться из средств создания подписи; данные, используемые для создания подписи, должны быть надежно защищены законным физическим лицом.

Квалифицированная цифровая подпись базируется не только на криптографическом алгоритме, но и на системе требований безопасности хранения и использования секретного ключа. Таким образом, сегодня в Украине производятся и используются как безопасные аппаратно-программные средства создания ЭЦП, так и средства создания ЭЦП с использованием вычислительных систем общего назначения, при этом повсеместно используются ключи, которые хранятся и транспортируются на флешках, CD, серверах и других носителях. Это прямое противоречие европейским законодательным нормам, поскольку безопасность данных, используемых для генерации цифровой подписи ключа, является основой основ в вопросе ЭЦП. Опубликованный проект закона об электронных доверительных услугах содержит прямые требования безопасности к средствам создания квалифицированных ЭЦП.

Надеюсь, что и в ходе гармонизации международных технических стандартов требования безопасности к средствам создания квалифицированных ЭЦП будут отражены корректно, а пользователи, в частности, банки, будут пользоваться безопасными средствами создания квалифицированных ЭЦП в тех системах, где это целесообразно.

директор по аудиту, консалтингу и сертификации ООО «Центр Системных Интеграций (SICenter)»

Ирина ИВЧЕНКО

Прежде всего хочу отметить, что в системе электронных платежей Украины используются средства формирования ЭЦП, полностью соответствующие требованиям европейских норм для квалифицированной ЕЦП, – секретный ключ не покидает защищенного носителя и подпись формируется внутри этого носителя. На основе Закона Украины «О Национальном банке Украины» с учетом особенностей обработки платежных документов Национальный банк Украины формирует требования по защите платежных документов. Целью создания Удостоверяющего центра для банковской системы Украины было именно обеспечение возможности клиенту использования одного ключа ЭЦП для работы с любым или несколькими банками. Использование для этих целей ключей и услуг существующих центров сертификации ключей было невозможно с момента их создания и ситуация практически не изменилась до настоящего времени из-за отсутствия интероперабельности. В настоящий момент все технические вопросы работы Удостоверяющего центра решены. Осталось решить вопросы изменения форматов платежных документов, привести форматы в соответствие с форматами системы платежей Евросоюза.

В европейских странах электронная цифровая подпись используется намного реже, нежели в Украине, в основном при обмене конфиденциальной информацией между государственными органами. Я не думаю, что сейчас стоит открывать обширную кампанию по переводу документов в электронный формат и активное использование ЭЦП, тем более, что это сопровождает ряд существенных преград. В первую очередь следует четко определить правила использования ЭЦП для различных типов документов и информации, содержащейся в них, проанализировать необходимую степень защиты, в том числе наличие ЭЦП квалифицированной или неквалифицированной, либо просто электронной подписи. Очень важно также отметить низкий уровень осведомленности, а следовательно и незнания, когда и зачем используется ЭЦП. Также отдельный вопрос – готовы ли государственные, силовые и судебные органы к работе с электронными документами.

Алексей СИРАКОВ

координатор Комитета по вопросам банковской инфраструктуры и платежных систем Ассоциации «Независимая ассоциация банков Украины»

В современных условиях наличие в банковской сфере инструмента, который приравнивает документы в электронном виде к подписанным собственноручно, более чем очевидно и необходимо: нет необходимости тратить сотни тысяч гривен на обеспечение хранения документов в бумажном виде; при этом резко сокращаются затраты на согласование, подписание, отслеживание версий, поиск и хранение документов; в прошлое уходят такие понятия, как утеря документа, затраты на его восстановление (при этом необходимо учитывать как человеческие, так физические ресурсы); наличие усиленной (или в новом проекте закона – «квалифицированной») электронно-цифровой подписи клиентов банка также позволит им значительно облегчить свою работу, ведь для проведения любой операции с банком (начиная от заключения договора и заканчивая проведением финансовых операций) клиенту понадобиться всего один ключ, полученный в аккредитованном (квалифицированном) центре сертификации ключей. Также этим ключом можно будет пользоваться для работы с любым банком Украины, то есть связки «брелоков» с ключами от систем клиент-банк, которые есть почти у каждого бухгалтера крупной компании, исчезнут. И этот самый ключ можно будет использовать и для работы с госорганами (отправка отчетности, получение справок и т.д.).

Однако на этом пути есть несколько существенных проблем: 1. Отсутствие единых форматов данных от ЦСК разных производителей и параметров электронного документа, хотя все системы работают на одних и тех же стандартах, но пути их реализации значительно разняться; 2. Отсутствие описания процесса вывода электронного документа на печать с отображением ЭЦП; 3. Отсутствие законодательного требования об обязательном приеме электронных документов государственными и судебными органами (которое возникает из-за нерешенности 1-го и 2-го вопросов).

При этом следует учитывать, что решение первого вопроса еще не реализовано в странах Европейского Союза, а разница в реализации стандартов приводит к непониманию одной системы ЭЦП системой другого производителя.

Тарас КАЧКА

и.о. президента Американской торговой палаты в Украине

Фінансові організації – члени Американської торгівельної палати дуже зацікавлені в тому, щоб Україна якомога більш інтенсивно впроваджувала стандарти ЄС та міжнародні системи електронних ключів. На сьогодні існують декілька суттєвих проблем на шляху розвитку та поширення електронного цифрового підпису в Україні. По-перше, це відсутність фактичного функціонування Засвідчувального центру Національного банку України та можливості використовувати іноземні технології електронних ключів в Україні (наприклад, 3SKeySolution). По-друге, це недосконаліть інтероперабельності вже існуючих рішень, а також витратність міжнародних технологій для локальних банків, що є відмінним орієнтиром розвитку від банків з іноземним капіталом.

В ходе панельной дискуссии представители государственных органов и финансовой элиты страны выделили и обсудили наиболее актуальные и проблемные вопросы, касающиеся внедрения и развития функционирования ЭЦП в Украине, а также внесли собственные предложения по улучшению ситуации.

Понимая важность и серьезность задач, с необходимостью решения которых ежедневно сталкиваются многие банки, страховые, кредитные и лизинговые компании, редакция международного журнала «Банкиръ» создает экспертную рабочую группу, которая будет способствовать поиску новаторских решений в этом вопросе на основе широкого партнерства с органами государственной власти и финансово-кредитными учреждениями.

Мы искренне надеемся, что она станет отличной площадкой для широкой кооперации регуляторов, органов государственного управления, отечественных компаний и их европейских партнеров.

Панельная дискуссия «Особенности внедрения электронной цифровой подписи в Украине», прошедшая в рамках IV Международной конференции «Безопасность финансово-кредитных учреждений: новые вызовы – новые решения – 2015», – лишь первый шаг на долгом пути координации и консолидации усилий банковских и финансово-кредитных учреждений в вопросах внедрения ЭЦП. Приглашаем всех заинтересованных к участию в дальнейших дискуссиях для поиска наиболее эффективных решений и принятия необходимых изменений в законодательстве в соответствии с европейскими и международными требованиями. ■

Записал Егор ЕРШОВ