Найти и обезопасить в интернет-пространстве

Вредоносным кодам, вирусам и мемам специалисты Беларуси и России противопоставят комплексную защиту

Сегодня мы являемся свидетелями и участниками стремительных перемен, когда цифровые технологии активно влияют на жизнь человека и общества, открывая новые перспективы для экономического, социального и культурного развития. Цифровая трансформация экономики признана национальным приоритетом и в Республике Беларусь, и в Российской Федерации. Однако при создании благоприятных условий для цифровизации разных сфер деятельности страны неизбежно сталкиваются с вызовом, который им в одиночку не преодолеть. Речь идет о безопасности цифрового пространства и угрозах, которым оно может подвергаться. Среди тем, требующих постоянного внимания, – совершенствование информационной безопасности Союзного государства и национальных систем защиты информации на основе технической защиты, криптографии, стандартизации в области информатизации, подготовки кадров. Наиболее сложные проблемы в области комплексной защиты информации включены в научно-техническую программу Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств – участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»). Многие из них обсуждались специалистами Беларуси и России на XXIV научно-практической конференции «Комплексная защита информации».

Действовать на опережение

Четвертая технологическая революция повлекла за собой глобальный процесс коренных преобразований по становлению нового уклада мировой экономики и нового цифрового коммуникационного пространства. Мир переходит к цифровому мышлению. Новая среда базируется преимущественно на виртуальном ресурсе, основой для которого выступает информация. Теперь и на интернет распространяются традиционные проблемы ее защиты.

Для виртуального пространства сегодня актуальна не только защита аппаратно-программных платформ от компьютерных атак в части нарушения конфиденциальности, целостности и доступности, функциональной устойчивости, но и борьба с новыми информационными угрозами, направленными на сознание человека и сообщества в целом.

В марте 2019 года Президент Александр Лукашенко подписал постановление Совета Безопасности «О концепции информационной безопасности Республики Беларусь». Документ предусматривает комплексный подход в обеспечении информационной безопасности, служит основанием для формирования государственной политики, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере. А 19 апреля 2019 года, обращаясь с Посланием к белорусскому народу и Национальному собранию, Президент Беларуси подчеркнул, что ситуация давно

требует принятия решительных мер по укреплению информационной безопасности страны, и в первую очередь это касается Глобальной сети.

– Коммуникационные технологии в Беларуси развиваются активно, – констатировал А.Г. Лукашенко. – В 2018 году по этому показателю наша страна заняла 38-е место почти из 200 государств. Но эта технологичность открывает новые возможности и для преступного вмешательства, несанкционированного получения и использования данных, в том числе личных… Мы должны не только принимать оперативные меры реагирования на информационные угрозы, но и действовать на их упреждение и опережение.

Очевидно, что в условиях осложнения международной обстановки и активизации террористической деятельности усиливаются угрозы информационной безопасности Союзного государства, связанные с деятельностью иностранных государств, преступных сообществ и отдельных лиц в таких сферах, как государственное управление, банковская деятельность, эксплуатация автоматизированных систем управления технологическими процессами критически важных объектов, обработка персональных данных. В связи с этим одним из важных направлений является предупреждение и нейтрализация угроз информационной безопасности общих информационных ресурсов Республики Беларусь и Российской Федерации.

Государственный секретарь Союзного государства Григорий Рапота в приветствии от имени Постоянного Комитета назвал XXIV научно-практическую конференцию «Комплексная защита информации» ведущей площадкой двух стран для обсуждения вопросов комплексной защиты безопасности научными, образовательными, производственными и государственными учреждениями России и Беларуси. Он отметил, что значение форума трудно переоценить, ведь результаты его работы широко используются для совершенствования информационной безопасности и систем защиты информации Беларуси и России и в иных смежных сферах деятельности.

В 2018 году начата реализация четвертой по счету программы «Совершенствование системы защиты информационных ресурсов Союзного государства и государств – участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»). Цель ее состоит в опережающем развитии технологий защиты информационных ресурсов Беларуси и России в условиях складывающейся вокруг этих государств геополитической обстановки.

Организаторами научно-практической конференции, проходившей в конце мая в Витебске, выступили Постоянный Комитет Союзного государства, Аппарат Совета Безопасности Российской Федерации, Парламентское Собрание Союза Беларуси и России. Среди ее участников – ведущие ученые и специалисты научно-исследовательских организаций Беларуси и России, представители министерств обороны, внутренних дел, связи и информатизации, Оперативно-аналитического центра при Президенте Республики Беларусь.

На форуме обсуждались новые риски, вызовы и угрозы, порожденные стремительным развитием информационного общества, которые сегодня напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Также в центре внимания были приоритетные для Союзного государства решения в сфере технической защиты информации, криптологии, криминалистики, в том числе разрабатываемые в рамках государственных и союзных программ инновационные методы и технологии защиты информационных ресурсов и систем.

На пленарных и секционных заседаниях белорусские и российские коллеги делились накопленным опытом по совершенствованию системы защиты инфор-

мационных ресурсов Союзного государства, профилактике информационного терроризма в условиях формирования глобального IT-общества, классификации угроз безопасности для киберфизических систем, вместе анализировали возможные каналы утечки информации в волоконно-оптических линиях связи. Вспомнили также историю и достижения белорусской и российской школ защиты информации.

Как подчеркнул в интервью обозревателю журнала «Беларуская думка» один из ведущих ученых в области криптологии – директор НИИ прикладных проблем математики и информатики БГУ, научный руководитель кафедры математического моделирования и анализа данных БГУ, доктор физико-математических наук, профессор, член-корреспондент НАН Беларуси Юрий Харин, актуальность тематики конференции из года в год только возрастает.

– Мир в XXI веке вынужден существовать не только в реальном, но и в цифровом формате, – отметил Юрий Семенович. – У каждого человека, организации и даже страны фактически есть двойник в цифровом пространстве. Только если в реальной жизни существуют действенные законы, нормативные документы, которые регламентируют, как жить, что можно или нельзя, то в виртуальном информационном пространстве аналогичных документов практически нет. Поэтому, наряду с такими положительными моментами, которые дает нам цифровой мир, возникают и неприятные. Например, когда персональные данные человека или же секретные документы предприятия могут быть открыты для общего доступа. И сейчас действительно такие нарушения фиксируются. В частности, уже разбираются в суде дела о взломе персональных сайтов. Есть подобные нарушения и на международном уровне: иногда государства начинают обвинять друг друга в кибератаках в ходе выборов в другой стране. И уровень такого межстранового противостояния в информационном пространстве не снижается.

Криптографическая защита

Рассматривая проблему перехода экономики в цифровой мир, заместитель директора по стратегическому развитию Института комплексной безопасности и специального приборостроения Российского технологического университета МИРЭА (РТУ МИРЭА) кандидат технических наук Виталий Григорьев заострил внимание на технологиях блокчейн и биткоин, позволяющих взглянуть по-новому на такие фундаментальные понятия, как ценообразование, соотношение цифровых и бумажных валют, меры юридического доверия, беспосредническая электронная торговля товарами и услугами и т. д. По мнению ученого, все идет к тому, что фундаментальные многовековые основы традиционной монетизированной «бумажной» экономики будут в корне пересмотрены.

– Уже сегодня технология блокчейн обеспечивает новый «цифровой формат доверия», вследствие чего эта криптоплатформа представляет интерес для представителей самых разных сфер, – считает Виталий Робертович. – Финансовому сектору она дает возможность организации нового и безопасного коридора для проведения клиентских операций. А государственным органам – хранения, например, данных кадастра. По идее, используя эту криптоплатформу, любой пользователь может передать другому сведения в зашифрованном виде, не опасаясь, что эта информация будет перехвачена и использована злоумышленниками. К сожалению, нельзя сбрасывать со счетов, что такой возможностью могут пользоваться и деструктивные асоциальные группировки – террористические организации, криминалитет, экстремисты. Нам надо быть готовыми к такой угрозе.

Криптографическая защита информации по-прежнему является одним из самых надежных и проверенных способов. Активно развиваются и ее новые направления – квантовая криптография, гомоморфное шифрование для облачных и виртуальных платформ, легковесная

Задачи информационного противодействия пропаганде терроризма и экстремизма в Сети интернет

- Выявление фактов пропаганды террористической и экстремистской деятельности
- Фильтрация вредоносного контента
- Информационное обеспечение государственных органов власти
- Блокирование содержимого интернет-ресурсов террористической и экстремистской направленности посредством использования законодательства
- Распространение информационных материалов антитеррористического и антиэкстремистского характера

криптография для защиты киберфизических систем и интернета вещей.

Интересно, что эта наука считалась одной из самых закрытых до конца XX века, даже упоминание слова криптография в открытой печати было запрещено. Ее преимуществами пользовались в основном силовые структуры и представители дипломатического корпуса. Возможно, в связи с этим премьер-министр Великобритании У. Черчилль как раз и говорил: «Тот, кто владеет информацией, тот владеет миром». А в наше время криптография стала необходимым элементом электронного документооборота, где защита персональных данных обеспечивается методом шифрования. Впрочем, как и в процессе обеспечения мобильной связи, где информация, которую мы передаем на участке от телефона до базовой станции, тоже вначале шифруется определенным алгоритмом, а на выходе – расшифровывается.

– Электронная цифровая подпись, шифрование, хеширование, аутентификация – всё это алгоритмы, которые относятся к криптографии, – пояснил Ю. Харин. – Криптография замечательна тем, что она базируется на математике и позволяет гарантировать стойкость защиты информации. То есть если выразить информационное сообщение закодированной последовательностью и отправить по открытому каналу, например по интернету, ваш противник, даже при наличии самого мощного компьютера, расшифрует цифровое выражение данного послания лет через 50.

В большом блоке актуальных направлений по комплексной защите информации ученые и специалисты Беларуси и России приоритетную позицию все же оставляют за технической защитой, в том числе от побочных электромагнитных излучений. В современных условиях это, можно сказать, достаточно традиционная защита от несанкционированного доступа к различным компьютерным ресурсам, включая виртуальные смарт-карты, в частности с помощью пароля. Актуальна и защита от утечек информации по телефонным и компьютерным каналам. Впрочем, для получения секретных данных злоумышленники готовы и к более инновационным маневрам. Так, например, специально оборудованная машина, стоящая где-то в окрестностях офиса, может получать важную информацию… по вибрации стекол этого помещения.

По словам Ю. Харина, сегодня набирает популярность достаточно новый способ защиты информации – стеганографический. Такая двухуровневая защита

состоит в том, что скрывается не только само сообщение, но и сам факт его передачи. Защита достигается встраиванием зашифрованного сообщения в некоторый «безобидный» компьютерный файл-контейнер, например фотографию.

– Россия традиционно ведет гораздо большее количество научных исследований в данной области, поэтому сотрудничество с российскими учеными для нас представляется очень важным, – подчеркнул белорусский исследователь. – Во многом опираясь на опыт и показательные результаты наших коллег в области защиты информации, Беларусь разработала свою национальную криптографию, свои стандарты защиты информации.

За многие годы работы между белорусскими и российскими учеными и специалистами, как отметил Ю. Харин, сложилось не просто хорошее взаимопонимание, но настоящая научная дружба:

– Показательно в этом отношении сотрудничество по реализации программ Союзного государства. Создан серьезный фундамент в области комплексной защиты информации. Практическое применение инноваций позволяет нам справляться с киберугрозами и кибератаками, используя самые современные средства шифрования, не допускать утечки информации, обеспечивая стратегически важную для наших стран информационную безопасность. На новом, более высоком, уровне даст возможность решать данные задачи реализуемая в настоящее время научно-техническая программа Союзного государства «Паритет». Конечно, хотелось бы, чтобы больше было таких совместных проектов.

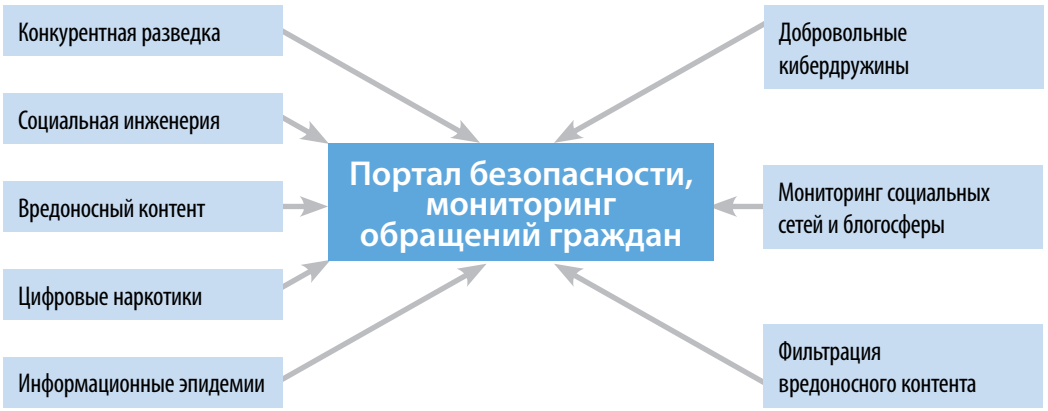
Напомним, что данной программой предусмотрено создание научно-технических условий, необходимых для реализации мер по предупреждению и нейтрализации угроз безопасности информации в автоматизированных системах управления технологическими процессами критически важных объектов Республики Беларусь и Российской Федерации – с 39 % в 2018 году до 61 % в 2022; по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), в информационных системах Союзного государства – с 59 % в 2018 году до 83 % в 2022.

По «цифровому» следу

Рассказывая об инструментах, используемых злоумышленниками в Сети для кибератак, главный специалист по защите информации ОАО «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления», доктор технических наук, профессор Михаил Бобов привел в пример наиболее известные: Фишинг, Троян, DDoS-атака, Ботнет, Backdoor, Червь, Руткит, Фрод, Флуд (Flood). Все это многообразие предназначено для достижения основной цели – проникновения в защищаемую инфокоммуникационную среду и установления над ней контроля.

Совершенное в киберпространстве преступление выявить и расследовать чрезвычайно сложно. Ведь преступник в большинстве случаев является высококвалифицированным IT-специалистом со сформированными профессиональными навыками «заметания следов». К тому же преступления им совершаются скрытно, относятся к неочевидным преступным деяниям и имеют длящийся характер. Поэтому здесь нужны отлично подготовленные профессионалы, способные найти злоумышленника по «цифровому» следу.

Как отметил начальник отделения Управления по раскрытию преступлений в сфере высоких технологий (Управление «К») Министерства внутренних дел Республики Беларусь Сергей Мирук, выявление, раскрытие и расследование преступлений в сфере информационной безопасности – это сложный комплекс взаимосвязанных мер оперативных и следственных подразделений, а также различных структур государственного и негосударственного секторов. И осуществляется он не в виртуальном пространстве, а на конкретной территории той или иной страны и конкретными специ-



◀ Система защитных рубежей

алистами, взаимодействующими между собой на международном уровне.

– Анонимность, быстродействие, трансграничность – именно эти факторы прельщают злоумышленников в Сети интернет, и они же осложняют процесс идентификации и привлечения нарушителей закона к установленной ответственности, – утверждает Сергей Валерьевич. – Кроме того, в последнее время наблюдается такая тенденция: киберпреступления приобретают групповой характер либо же киберпреступник использует большое количество компьютеров.

Согласно полученным данным, криминогенная обстановка в Республике Беларусь красноречиво свидетельствует о необходимости активного противодействия киберпреступности. Не может не вызывать тревоги такая динамика: если в 2016 году в сфере высоких технологий было зарегистрировано 2471 преступление, то в 2017 – 3099, в 2018 – 4741, а за первый квартал 2019 года – уже 2124 преступления.

Представитель МВД отметил, что значительное количество киберпреступлений носит трансграничный характер, поэтому международное сотрудничество, повышение доверия и оперативности обмена данными как между правоохранителями, так и глобальными поставщиками интернет-услуг имеют большое значение. Злоумышленники с целью сокрытия своего истинного местонахождения и следовой картины совершаемого преступного деяния используют различные формы и методы анонимности, анонимные IP-адреса, TOR, VPN-сервисы, криптовалюту, обезличенные либо оформленные на подставных лиц банковские платежные карты, кошельки электронных платежных систем и иных учетных записей. Как правило, они идут на совершение киберпреступлений на территории иностранных государств, в отношении иностранных граждан и субъектов хозяйствования. В отдельных случаях могут привлекать к преступной деятельности жителей разных стран, а грузы – похищенное имущество, орудия преступлений – перемещают с использованием анонимных сервисов по оказанию транспортных услуг и т. д.

– С учетом роста количества выявляемых киберпреступлений увеличивается и число обращений в правоохранительные органы иностранных государств, – констатировал С. Мирук. – Так, в 2016 году нами было направлено 387 таких обращений, в 2017 – 915, в 2018 году – уже 1123. Из них соответственно 272, 802 и 1064 в адрес национальных контактных пунктов России. Данное обстоятельство напрямую связано с использованием потерпевшими и злоумышленниками сетевых ресурсов и технологий как зарегистрированных, так и находящихся на территории Российской Федерации. В связи с этим очевидно, что качество работы подразделений МВД Беларуси в сфере высоких технологий по раскрытию преступлений против информационной безопасности существенно зависит от оперативного обмена информацией с

зарубежными партнерами, в первую очередь российскими.

Киберпреступность интернациональна. И в борьбе с ней могут быть эффективны только совместные усилия многих стран. В настоящее время действует международная сеть национальных контактных пунктов «24/7», которая позволяет оперативно обмениваться информацией о готовящихся, совершаемых либо совершенных преступлениях в киберпространстве, а также запрашивать необходимую для проведения оперативно-разыскных мероприятий техническую и иную информацию из аналогичных подразделений правоохранительных органов государств – участников информационного обмена.

Сеть объединяет более чем 70 стран, среди которых США, Германия, Великобритания, Испания, Швеция, Бразилия и многие другие. Как рассказал С. Мирук, Бюро специальных тактических мероприятий (Управление «К») МВД России и Управление «К» МВД Беларуси также входят в международную сеть национальных контактных пунктов «24/7».

Представители правоохранительных органов Беларуси и России особо подчеркивают важность объединения усилий специалистов двух стран в борьбе с киберпреступностью в условиях постоянного роста ее динамики и масштабов, увеличения причиняемого ущерба государственным структурам, юридическим и физическим лицам. Киберугрозы и киберпреступления представляют серьезнейшую проблему для общества, и борьба с ними является актуальной задачей для правоохранительных органов. Особенно важно принятие мер по своевременному установлению лиц, совершивших преступные деяния, и получению доказательств, подтверждающих совершение правонарушения в Глобальной сети.

По словам сотрудников одной из важнейших спецслужб нашей страны – Оперативно-аналитического центра при Президенте Республики Беларусь, существенным подспорьем для обеспечения более совершенной защиты информации сегодня выступают программно-аппаратные комплексы для выявления и локализации радиопередающих средств технических систем несанкционированного съема информации и ведения мониторинга радиоэфира, внедренные в практику в Беларуси по результатам завершенной программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий на 2011–2015 годы». С использованием научно-технических разработок подготовлена технологическая база к серийному выпуску устройств криптографической защиты информационного обмена в вычислительных сетях.

Вирусы сознания

«В прежних войнах важным почиталось завоевание территории. Впредь важнейшим будет почитаться завоевание душ во враждующем государстве». На этой цитате полковника Генерального штаба Российской императорской армии, одного из крупнейших военных теоретиков XX века профессора Евгения Месснера не случайно акцентировал внимание заместитель директора по стратегическому развитию Института комплексной безопасности и специального приборостроения РТУ МИРЭА В. Григорьев.

– В эпоху глобализации, ослабления государственных границ, развития средств коммуникации важнейшим фактором стало изменение форм разрешения межгосударственных противоречий, – подчеркнул Виталий Робертович. – В современных конфликтах все чаще акцент смещается в сторону используемых методов борьбы – комплексного применения политических, экономических, информационных и других невоенных мер, реализуемых с опорой на военную силу. В то же время с их помощью достигаются политические цели с минимальным вооруженным воздействием на противника. Преимущественно за счет подрыва его военного и

Создание систем мониторинга и анализа социальных сетей, что обеспечит:

- получение комплексного представления о текущей ситуации в конкретном регионе или государстве, выделение и оценку основных индикаторов, указывающих на нарастание социальной напряженности, прогнозирование динамики развития кризисных тенденций, оценку политических настроений населения;
- выявление террористических сетей (ТС) и экстремистских сетей (ЭС) (структуры сети, степени связности узлов, диаметра сети и т. д.);
- отслеживание идей, концепций, оппозиционных настроений, информационно-пропагандистских кампаний, слухов и дезинформации, распространяемых в социальных сетях, оценку степени их влияния на аудиторию, определение источников распространения информации, выявление иерархической структуры и географии протестного движения, прогнозирование времени начала протестных выступлений;
- наблюдение за деятельностью отдельных личностей, сетевых сообществ и общественных организаций, оппозиционных по отношению к политике правительства;
- составление досье на интересующих участников социальных сетей (область интересов, привычки, психологические особенности и т. д.) с целью безличного изучения потенциальных кандидатов на вербовку, объектов проникновения, секретоносителей, оппозиционных активистов, представителей бизнеса и СМИ и т. д.;
- выявление лиц и группировок, подозреваемых в подготовке террористических актов.

экономического потенциала, с применением информационно-психологического давления, активной поддержки внутренней оппозиции, партизанских и диверсионных методов. В качестве главного средства используются «цветные революции», которые, по мнению инициирующих их сторон, должны привести к ненасильственной смене власти в стане оппонента. По сути, любая «цветная революция» – это государственный переворот, организованный извне. А в основе лежат информационные технологии, предусматривающие манипуляцию протестным потенциалом населения в сочетании с другими невоенными средствами.

Как отметил эксперт, формы проявления «информационного терроризма» весьма разнообразны: от действий по дезорганизации автоматизированных информационных систем, создающих опасность гибели людей и причинения значительного имущественного ущерба, до угрозы или реального применения физического насилия, запугивания и дестабилизации общества и таким образом оказания влияния на население или государство. Возможно широкое и многоплановое воздействие на социум и индивида различными элементами деструктивных влияний с акцентом на мировоззренческие социокультурные стереотипы в поведении, умонастроении и образе жизни людей.

– Используя в своих целях информационные ресурсы интернета, экстремистские организации ведут, по сути, борьбу за души и сознание подрастающего поколения и молодежи, – утвержда-

ет В. Григорьев. – Идет подмена и перепрограммирование нравственных ценностей, разрушение социокультурных традиций, формирование бездушных, покорных управляемых биороботов. Как технологии информационного терроризма задействуются различные ресурсы – блоги, социальные сети, ЖЖ, форумы и т. д., также компьютерные игры, цифровые наркотики, психокоммутативные гаджеты, мемовирусы нового поколения, управляемые «малые миры» в виртуальных социальных сетях.

Особо востребованы сегодня у злоумышленников, как отмечают специалисты, различные способы психологического воздействия. К ним, кстати, относятся и вирусы сознания, так называемые мемы. В Глобальной сети они, как правило, представляют собой некую информацию – отдельную фразу, мелодию, текст, медиафайл – добровольно передаваемую пользователями друг другу. Обычно это делается в целях развлечения, но этим же способом может распространяться и другая информация, в том числе провокационного или злонамеренного характера. Зачастую средой для распространения мемовируса являются блогосфера и форумы, однако мемы могут также тиражироваться с помощью мессенджеров, электронной почты и даже выходить за пределы интернета, например, попадая в СМИ.

Работа по информационному противодействию терроризму и экстремизму в интернете, по мнению В. Григорьева, не исключает фильтрации вредоносного контента, блокирования содержимого интернет-ресурсов террористической и экстремистской направленности посредством использования законодательства и распространения материалов антитеррористического и антиэкстремистского характера.

Неординарная образовательная среда

Развитие новой синергетической отрасли информационной среды жизнедеятельности человека в виде взаимосвязанных объектов защиты цифровой экономики, цифрового социума, интернета вещей, критических информационных инфраструктур, других промышленных и бытовых киберфизических систем требует развертывания масштабной подготовки грамотных, высокопрофессиональных специалистов в области обеспечения информационной безопасности. Это отмечали все участники научно-практической конференции.

– Учитывая, что сегодня в мире идет переход на цифру, потребуется массовая подготовка специалистов в области открытой криптографии, прикладного программирования и искусственного интеллекта, – утверждает директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА Владимир Лось.

За последние 10–15 лет потребность в профессионалах по защите информации не стала меньше. И это несмотря на то, что теперь подготовку по данным специальностям в России ведут более чем 120 вузов. Спрос удовлетворяется всего лишь на 50 %. Подготовка специалистов по защите информации сегодня становится важным условием решения проблем, стоящих перед российским технологическим рынком в части нормативно-технического регулирования перспективных технологий: интернета вещей, больших данных, умных городов и т. д.

– Анализ текущего состояния и перспектив обеспечения информационной безопасности России показывает, что необходима целенаправленная подготовка высококвалифицированных кадров, способных эффективно решать постоянно увеличивающийся комплекс задач по гарантированной защите современных телекоммуникационных и информационных технологий, составляющих инфраструктуру информационного базиса государственных систем управления, – подчеркнул В. Григорьев. – Информационная безопасность России во многом определяется именно стратегией подготовки специалистов в области новых информационных технологий, опреде-

ляющих независимость государства с точки зрения своевременного адекватного ответа на стратегические вызовы в XXI веке.

– Существенно возросли требования, предъявляемые к новому поколению специалистов, в силу беспрецедентной сложности указанных задач при постоянном росте внешних и внутренних угроз информационной безопасности, – поддерживает коллегу белорусский ученый Ю. Харин. – Здесь нужна неординарная образовательная среда, включая виртуальные лаборатории и тренинги по противодействию проникновению, с захватом, скажем, баз данных, использование новейших программных продуктов IT-сферы. Ведь специалист должен быть на шаг впереди злоумышленников в Сети, которые тоже в своем роде профессионалы. Кроме того, имеется тенденция к расширению круга задач, требующих неотложного решения с позиций защиты информации. Например, противодействие «информационному оружию», защита критических государственных и экономически значимых инфраструктур, разработка конверсионных технологий двойного назначения, импортозамещение и т. д.

К слову, в учебном процессе БГУ используются созданные в рамках предыдущей союзной программы «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий на 2011–2015 годы» электронные учебные пособия по теории вероятностей, математической статистике, теории конечных автоматов; высокоскоростной малогабаритный генератор случайной числовой последовательности гарантированного качества на физическом источнике шума; программное обеспечение встраивания цифровых водяных знаков в графические изображения, видеофайлы, аудиофайлы и мультимедийные файлы.

Улучшение организации процесса подготовки и переподготовки специалистов по информационной защите можно рассматривать как задачу государственной важности. И нет сомнений, что, проводя в рамках конференции Школу молодых ученых, Постоянный Комитет Союзного государства делает значимое дело. Прежде всего потому, что начинающим специалистам предоставляется возможность увидеть свою будущую профессию через людей, имеющих высочайший авторитет в области комплексной защиты информации. Также они могут предложить свою уникальную идею в IT-сфере. Надо сказать, что такие высококвалифицированные кадры становятся все более востребованными в пространстве социального, экономического и финансового взаимодействия в многоагентных сетевых многосвязных структурах формирующегося глобального цифрового общества.

Интенсивное внедрение IT-технологий привело к тому, что информационный ресурс является сегодня таким же богатством, как производственный и людской потенциал. Следовательно, обеспечение информационной безопасности личности и государства – важнейший фактор и необходимое условие, положительно влияющие на стабильное социально-политическое и экономическое развитие Беларуси, России и Союзного государства в целом. Для специалистов в сфере комплексной защиты информации сегодня важно оценить возможные риски и угрозы в области информационной безопасности, просчитать алгоритмы действий по предотвращению или минимизации ущерба в случае нарушения функционирования информационно-телекоммуникационных систем органов власти и организаций Союзного государства. Решение данных задач будет способствовать сохранению научно-технического потенциала в наших странах, развитию производства конкурентоспособных технических программно-аппаратных и программных средств защиты информации в Беларуси и России и обеспечению комплексной надежной защиты одного из самых востребованных в наше время стратегических ресурсов современного общества – информации.

Снежана МИХАЙЛОВСКАЯ