

Противопоставить киберугрозам комплексную защиту



Давно пора признать: мы живем в знаменательное время – начала цифровизации, становления глобального информационного пространства. Уже сейчас во многих странах оцифровывают все, что можно: медицинские карты, государственные базы данных, сведения образовательных учреждений. Однако наряду с достижениями в IT-области и активным переходом на цифру возникают проблемы обеспечения информационной безопасности личности, бизнеса и государства. Новые угрозы такого рода специалисты Беларуси и России не только изучают, но и стараются держать под контролем. Ежегодно, вот уже на протяжении 20 лет профессионалы в области систем защиты информации сверяют направления противодействия киберугрозам на международной научно-практической конференции «Комплексная защита информации». Важным подспорьем научному сопровождению и практическому воплощению проектов в данной области стала реализация трех программ Союзного государства, на подходе проект новой, названной «Паритет-2020».

Компьютер с вирусным иммунитетом

В последнее время все чаще случаются компьютерные инциденты в информационных системах разных стран. Классический пример: в июле 2010 года с использованием вируса Stuxnet были осуществлены атаки на десятки миллионов компьютерных систем в Китае, Индии, Иране. Установлено, что конечной целью создателей этой вредоносной программы являлись информационные системы Бушерской АЭС в Иране. К сожалению, не осталась вне опасных воздействий и наша страна: в течение 2010–2011 годов неоднократно фиксировались сбои в функционировании системы обработки безналичных расчетов банковских пластиковых карточек Банковского процессингового центра в Беларуси и даже многочисленные хакерские атаки на сайты белорусских государственных органов. Атакам подвергаются также социальные сети и коммерческие сайты.

Число преступлений, связанных с посягательствами на информацию, передачу данных, информационные тех-

нологии, которые совершаются в компьютерных сетях и системах, а также в интернете, растет в геометрической прогрессии. Вот и в 2017 году хакерские атаки обрушились на многие страны мира. По оценке известной российской компании «Лаборатория Касперского», работающей в сфере информационной безопасности, 12 мая было проведено 45 тыс. попыток взлома в 74 странах. При этом большая часть из них пришлась на Россию. На экранах зараженных компьютеров появлялись сообщения с требованиями злоумышленников. Надписи на мониторах гласили, что хакеры готовы разблокировать сети при получении 300 долларов в кибервалюте – биткоинах. Согласно сообщению «Лаборатории Касперского», вирус, о котором идет речь, – программа-шифровальщик WannaCry. В мае нынешнего года под ее ударом оказались больницы, железные дороги, правительственные учреждения. Отражать атаки пришлось специалистам МЧС и Минздрава, Сбербанка и компании «Мегафон».

– Мир подошел к той черте, когда границы между государствами пере-

стали быть непреодолимыми не только для бизнеса и торговли, науки и образования, отдыха и развлечений, но и для терроризма, преступности, в том числе в сфере высоких технологий, – отмечает заведующий кафедрой технологий программирования факультета прикладной математики и информатики Белорусского государственного университета, доктор технических наук, профессор Александр Курбацкий. – Угрозам подвергаются самые разные информационные системы: как государственные, так и коммерческие. Глобальная тенденция цифровизации заставляет нас реагировать на все эти вызовы и решать проблемы безопасности в цифровом мире.

По мнению профессора, одним из приоритетных направлений в обеспечении безопасности информационно-коммуникационных систем Республики Беларусь является развитие законодательства в этой сфере как основы организации работ всех заинтересованных государственных органов, предприятий и граждан. В целом над созданием комплексной защиты информации в цифровой среде в Беларуси и в России работают уже много лет. Однако проблему борьбы с вирусами не решить в формате одного государства, считает А. Курбацкий. Это потенциальное поле деятельности для специалистов в рамках Союзного государства, объединение усилий всех стран мира.

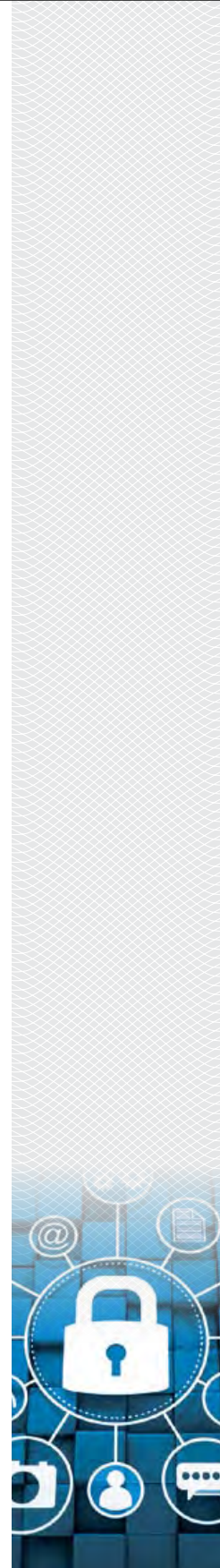
– Как правило, над проблемой противодействия вирусному заражению компьютеров работают мировые корпорации. Потенциал Беларуси в данной области, к сожалению, невелик, – отмечает А. Курбацкий. – На этом рынке в нашей стране, по сути, успешно пытается удержаться пока только одна частная компания «ВирусБлокАда». На государственном уровне разработок по антивирусной защите немного. Но это, в принципе, общемировая тенденция: как правило, антивирусные компании – представители частного бизнеса. Даже в США Агентство национальной безопасности, Пентагон, пользуются IT-разработками компаний негосударственного сектора.

Такая же картина в России или, к примеру, в Китае. Однако в этих странах действуют крупные компании с хорошим финансированием, работающие в области антивирусной защиты. Масштабные рынки – американский или китайский, даже российский, не сравнить с белорусским. Понятно, что вырастить более-менее профессиональной команде там гораздо проще, чем в Беларуси. В России около десятка фирм работают в данной сфере: та же известная во всем мире «Лаборатория Касперского», InfoWatch, «Доктор Веб» и другие. Есть предложения антивирусов и у других интеграторов кибербезопасности, но все это – дорогостоящие продукты.

Компьютерные вирусы в мире появляются едва ли не каждый день. Чтобы написать защитную программу, ситуацию нужно мониторить. Поэтому над ее созданием должна работать большая команда профессионалов.

– Следует учитывать, что преступления, связанные с посягательством на конфиденциальную информацию, имеют экспоненциальный рост, – отмечает директор Научно-исследовательского института прикладных проблем математики и информатики Белорусского государственного университета, заведующий кафедрой математического моделирования и анализа данных, член-корреспондент НАН Беларуси Юрий Харин. – По данным американской компании IBM, каждую секунду в мире происходит 18 компьютерных преступлений. Кроме того, наблюдается и рост их разнообразия. Например, атаки компьютерных вирусов с целью блокирования или кражи конфиденциальной информации – тот же вирус-блокировщик WannaCry. А еще возможна криптоаналитическая атака для определения ключевой информации, подмена автора сообщения, подмена сообщения и др.

По мнению Ю. Харина, растущий поток компьютерных преступлений – это следствие становления глобального информационного пространства (цифрового мира), национального информационного пространства и корпоративных



информационных пространств. Цифровая информация становится все более высокоценным ресурсом и товаром. Ее объем растет тоже экспоненциально и, к примеру, в США к 2020 году он составит 7×10^{21} байт. Поэтому защита информации – важнейшая проблема национальной и международной безопасности.

– Когда мы говорим об атаках хакеров, следует понимать: проблема кроется не в том, что плохо работают антивирусные компании, а в том, что архитектура компьютера по модели Тьюринга уязвима изначально, – подчеркивает научный руководитель ОКБ САПР, заведующий кафедрой защиты информации Московского физико-технического института, доктор технических наук, профессор Валерий Коняевский. – Универсальный компьютер Тьюринга может выполнить любую программу – а значит, и вредоносную. Вот хакеры и паразитируют.

Вместе с тем, как рассказал российский ученый, в России недавно придумали компьютер, который не подвержен вирусному заражению.

– Хакеры больше не опасны, – утверждает В. Коняевский. – Вирусы используют архитектурную уязвимость компьютеров. – Бесполезно программными методами бороться с архитектурными изъянами. Понимая это, мы и предложили новый компьютер с вирусным иммунитетом. Если данное направление попадет в новую союзную программу, на наш взгляд, будет значимый результат. Ведь антивирусный компьютер – принципиально новое слово в IT-отрасли.

Профессионалы сверяют планы

Защита информации в цифровой экономике и информационных систем от ее утечки по скрытым каналам, разработка стойких криптографических алгоритмов и протоколов, гражданской электронной интеллектуальной карты (электронного паспорта), квантовая криптография, технология блокчейн и криптовалюты – эти и другие темы обсуждали участники XXII международной научно-

практической конференции «Комплексная защита информации». Форум проходил в мае 2017 года на базе Полоцкого государственного университета и собрал свыше 100 представителей Беларуси и России – это известные ученые, высококвалифицированные специалисты, а также представители ведущих организаций, осуществляющих деятельность в области защиты информации. Было заслушано более 70 докладов, в том числе и от школы молодых ученых.

История этого международного форума берет свое начало с 1997 года, когда в окрестностях Минска состоялась первая конференция. Проводить такие встречи ежегодно (поочередно в городах Беларуси и России) задумали для решения актуальных проблем обеспечения информационной безопасности только что родившегося Союзного государства и национальных систем защиты информации двух стран. Кстати, финансовую поддержку в организации конференций оказывает Постоянный Комитет Союзного государства.

Итогом многолетнего сотрудничества стало формирование эффективного механизма взаимодействия ведущих профильных экспертов в интересах выработки единого понимания основных вызовов и угроз в информационной сфере. И уже на протяжении длительного времени конференции способствуют консолидации усилий органов государственной власти, представителей научного, экспертного и бизнес-сообщества Беларуси и России на стратегически важном направлении. Директор Научно-исследовательского института прикладных проблем математики и информатики БГУ Ю. Харин подчеркивает, что с белорусской стороны наибольшая активность в организации форума принадлежит Оперативно-аналитическому центру при Президенте Республики Беларусь, Белорусскому государственному университету, Национальной академии наук Беларуси.

В последние пять лет тематика форумов сориентирована прежде всего на формирование трансграничного про-



странства доверия Союзного государства, противодействие киберпреступности. Среди направлений, требующих постоянного внимания, можно выделить техническую защиту информации, криптографию, стандартизацию в области информатизации, подготовку кадров.

Криптографический метод, по словам Ю. Харина, является основным, так как обеспечивает решение с гарантированной надежностью следующих задач защиты информации: конфиденциальность при ее передаче и хранении; аутентификация (подтверждение истинности) сообщения и отправителя; целостность сообщения при передаче и хранении; невозможность отречения от авторства.

На нынешнем этапе уже «открытой» компьютерной криптографии акцент сделан на электронном документообороте в информационном обществе.

Среди перспективных, считает белорусский исследователь, и новый способ защиты информации – стеганографический. Его суть состоит в том, что скрывается не только само сообщение, но и факт сокрытия сообщения. Это, так сказать, двухуровневая защита информации. Достигается она встраиванием зашифрованного сообщения в некото-

рый «безобидный» компьютерный файл, например, фотографию.

– Наиболее трудными в области комплексной защиты информации Союзного государства, требующими значительных финансовых ресурсов, являются проблемы, включенные в проект на 2017–2021 годы IV Союзной программы, – подчеркнул Юрий Харин. – Он называется «Совершенствование системы защиты информационных ресурсов Союзного государства и государств – участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» и включает обнаружение аномалий (в том числе вирусов и вредоносных кодов) в сетевом потоке автоматизированных систем управления криптографически важными объектами; разработку методов поиска недеklarированных возможностей в программном обеспечении; создание новых криптографических стандартов и методик испытания средства криптографической защиты информации и др.

Участники конференции по комплексной защите информации уверены, что результаты, полученные при реализации союзных программ, дают положительный экономический эффект и Беларуси,

▲ Участники
XXII научно-практической
конференции
«Комплексная защита
информации»
в Полоцке.
Май 2017 года

Беларуская
Думка

и России за счет предотвращения или минимизации ущерба от нарушения функционирования информационно-телекоммуникационных систем органов власти и организаций Союзного государства. Важным преимуществом совместной работы является экономия расходов двух стран на защиту национальных информресурсов и обеспечение безопасности информации в критически важных системах информационной инфраструктуры. Кроме того, решаются актуальные задачи: сохранение научно-технического потенциала в области защиты информации, развитие производства конкурентоспособных технических, программно-аппаратных и программных средств защиты информации.

– Когда много лет назад мы задумывали конференцию «Комплексная защита информации», то рассматривали ее как один из инструментов интеграционного движения в рамках Союзного государства, – отметил Валерий Конявский. – Планировали и делали так, чтобы за счет профессионального диалога ведомств с близкими задачами сближались и подходы к защите информации. Положительное движение в этом направлении было, но со временем данный тренд оказался несколько утраченным. На мой взгляд, сегодня необходимо больше усилий сконцентрировать на поиске совместных решений, которые могут применяться и в России, и в Беларуси. Такой интеграционный подход, безусловно, повысит эффективность союзных программ.

Интернет вещей

В последнее время все большую популярность набирает концепция «Интернет вещей». По прогнозам международной исследовательской компании IDC, вскоре подключенных к сети «умных» устройств будут десятки миллиардов. Поэтому не случайно некоторые специалисты уверяют: интернет вещей – это следующий кошмар информационной безопасности. Например, цифровая начинка умного дома крайне уязвима для хакерских вторжений.

– Чтобы обеспечить взаимодействие «вещей» нужны другие протоколы, защищенные нативно, – отмечает Валерий Конявский. – Иначе проблем будет немало. Пугать потребителей – дело не ученых, а маркетологов. Воздержусь и я от страшных рассказов о заговоре холодильников. Нужно с самого начала не надевать глупостей, а значит, к работам следует привлекать специалистов, а потом уж программистов. И не ждать, пока новая западная элементная база навяжет нам неконтролируемые решения.

Тем не менее нельзя отрицать очевидное: интернет вещей предоставляет возможность интеллектуальным предметам («умным холодильникам», «умным кухонным машинам», «умным автомобилям», «умным квартирам» и т. п.) иметь доступ в Сеть для выполнения своих функций.

– Наряду с огромными удобствами для человечества, это порождает и новые проблемы информационной безопасности, – поясняет Юрий Харин. – Проникая в программу управления такой «умной вещи», противник (террорист) может задать режим управления, опасный для людей. Безусловно, могут появиться и другие новые вызовы для информационной безопасности, которые сейчас еще не известны. Чтобы всегда быть к ним готовыми, есть одно универсальное средство – иметь достаточное количество квалифицированных специалистов по защите информации.

В Республике Беларусь и в Российской Федерации решению кадровой проблемы уделяется огромное внимание. В нашей стране специалистов по защите информации готовят в Белорусском государственном университете, Университете информатики и радиоэлектроники, Гродненском университете, Полоцком государственном университете. По новой специальности «методы и системы защиты информации, информационная безопасность» уже защищено 30 кандидатских диссертаций.

Вместе с тем есть еще и нерешенные проблемы в области подготовки высококвалифицированных специалистов по

компьютерной безопасности и защите информации, считает заведующий кафедрой технологий программирования факультета прикладной математики и информатики Белорусского государственного университета Александр Курбацкий. На белорусском рынке они менее востребованы, чем те же программисты, лучших из которых по окончании вузов забирают в IT-компании Парка высоких технологий.

– Так как базовая подготовка у специалистов по компьютерной безопасности аналогичная, и у них есть навыки по кодированию и тестированию программного обеспечения на основе несложных технологических платформ, многим проще уйти в обычное программирование и без проблем получить заведомо хорошо оплачиваемую работу, – пояснил профессор. – А между тем специалисты по защите информации – это, без преувеличения, штучный товар. Они обладают более обширными знаниями не только в программировании, но и в области компьютерной безопасности и криптографии.

Подчеркивая особенности подготовки профессионалов такого высокого уровня, Александр Курбацкий отмечает, что в сфере компьютерных технологий стратегически важно действовать с опережением. А это приходит через практические навыки в профессии, к примеру, участие в масштабных реальных проектах. К сожалению, пока таких заказчиков у БГУ катастрофически мало. Небольшим отечественным IT-компаниям сложно тягаться с мировыми корпорациями, поэтому они, как правило, не выигрывают тендеры на крупные заказы, соответственно – не нуждаются в новых специалистах высокого класса.

– Массовая цифровизация приводит к тому, что в IT-отрасли необходимо создавать и развивать все более сложные интегрированные системы, – рассказал Александр Курбацкий. – Основной подход: минимальная цена и желательно сдать систему под ключ. По условиям тендеров их проще разработать мировым вендорам. Так как у нас на вну-



треннем рынке универсальных игроков практически нет, мы отдаем все на откуп мировым компаниям-производителям, тем самым ослабляя внутренние компетенции и лишая работы отечественные компании. Соответственно, разрушаем и внутреннее образование в этой сфере, лишая студентов возможности участвовать в реальных масштабных проектах. Вот и сейчас на подходе крупный проект «Электронное здравоохранение» под кредит Всемирного банка с финансированием около 70 млн долларов. Но чтобы выиграть тендер и провести все работы под ключ в Беларуси, необходимо собрать в пул 5–6 отечественных IT-компаний.

Тем не менее определенные сдвиги в решении проблемы качественной практико-ориентированной подготовки специалистов в области защиты информации все же есть: в БГУ при поддержке Всемирного банка открывается новая двухлетняя магистратура по проектированию сложных интегрированных систем. Набирают архитекторов систем, аналитиков и специалистов по информационной безопасности.

– В наших планах не только предложить магистрантам сбор материала для будущей диссертации, но и реальную практику – участие в проектах по созданию сложных интегрированных систем, – подчеркнул А. Курбацкий. Тем более что спрос на такие проекты рас-

▲ На заседании конференции в Полоцке. Слева направо: заведующий кафедрой радиоэлектроники Полоцкого государственного университета В. Железняк, директор Научно-исследовательского института технической защиты информации А. Горбач, заведующий кафедрой защиты информации Московского физико-технического института, научный руководитель ОКБ САПР В. Коняевский. 2017 год

тет и в России, и в Евразийском союзе в целом. Намерены более тесно сотрудничать с российскими вузами. В частности, планируется, что с лекциями перед белорусскими магистрантами выступит профессор Валерий Коняевский. В перспективе стоило бы более широко развернуть полигон по отработке компетенций специалистов в области защиты информации в Союзном государстве.

– В России тоже не все гладко с подготовкой кадров в области компьютерной безопасности, – в свою очередь отметил Валерий Коняевский. – Потребности страны в специалистах по информационной безопасности – не менее 5 тыс. в год. Вузы выпускают – не более 3 тыс. Конечно, это очень мало, и специалистов не хватает. Притом готовятся в основном администраторы безопасности, а не разработчики. В Беларуси наблюдается другая картина – талантливые ребята с третьего курса начинают работать, уходят в программирование и забрасывают учебу. Поэтому на поприще подготовки высококвалифицированных кадров я вижу огромную потребность в нашей совместной работе. Организуя в рамках конференции по защите информации школу молодых ученых, Постоянный Комитет Союзного государства делает великое дело, предоставляя возможность молодым специалистам дать оценку своей будущей специальности, общаясь с людьми, имеющими высочайший авторитет в отрасли. И за это можно только поблагодарить Постоянный Комитет.

Интерес личный и трансграничный

На фоне масштабных проблем обеспечения информационной безопасности государства, крупного, в первую очередь транснационального, бизнеса, личная информационная безопасность человека часто остается в тени. Быстро погружаясь в виртуальный мир интернет-пространства, большинство из нас зачастую совершенно не заботится о безопасности. Эти вопросы сегодня активно обсуждают на мировых форумах,

много внимания им было уделено и на международной научно-практической конференции по комплексной защите информации в Полоцке.

Действительно, мы уже давно перенесли в интернет свою активность: оплата коммунальных услуг с помощью интернет-банкинга, проведение платежных операций через мобильный банкинг – этими сервисами сегодня активно пользуются даже представители старшего поколения. Добавьте к этому постоянный электронный обмен фото и видеoinформацией, которая выкладывается в переписке в тех же социальных сетях. При этом большинство пользователей забывают, что в цифровом мире особенно актуальна защита персональных данных.

– В Беларуси, как и в других странах, приняты законы по сохранению персональной информации, но многие ли из нас обращают на это внимание? – задается вопросом Александр Курбацкий. – В наше время у человека под любыми предложениями и разными способами постоянно вытаскиваются личные сведения. Уже сейчас явно заметны тенденции, когда все больше и больше личной информации заносится в онлайн-профайлы. Личная жизнь перестает быть тайной. Оформление дисконтных карт для получения скидок в магазинах связано с предоставлением анкетных данных, то есть персонализацией. Покупаете мобильный телефон – он тоже связан с оформлением сим-карты и вашими паспортными данными, значит, успешно вас идентифицирует. Как, впрочем, и электронная почта... Если подумать, то мы фактически сами раздаем свои персональные данные. И в просторах глобальной компьютерной сети о нас накапливается уйма информации. Мы даже не замечаем, как проявляется цифровой облик человека в этом цифровом мире. Тот же Google использует более 60 факторов для персонализации ваших поисковых результатов: тип компьютера, браузер, номера телефонов, IP-адреса и т. д.

К сожалению, многие пользователи не понимают, какие опасности существу-



ют. Государство, пытаясь защитить своих граждан, как правило, запаздывает, а в этой области все очень быстро меняется. В рамках Союзного государства также есть программы защиты информации, но преимущественно государственной.

– Профессионалы знают, как защитить себя и свою информационную систему, а общество – не знает, – считает Валерий Конявский. – Значит, в новой Союзной программе должен появиться раздел по популяризации новых подходов. Это будет правильно.

Кстати, на повестке дня у профессионалов еще одна важная проблема, которую предстоит решить: учитывая, что в компьютерном мире объекты глобальны, представляется очень сложным жестко выстроить цифровые границы территориально. К примеру, совершено киберпреступление, но на какой территории, под юрисдикцию специалистов какой страны оно подпадает? Сервер, с которого киберпреступник атакует, может находиться где угодно. В этой связи военные США, к примеру, считают необходимым приравнять информационное пространство к другим видам – морскому, воздушному, наземному. Следовательно, угроза в информационном пространстве будет равнозначна любой иной угрозе. Но если утвердить такой подход в международном праве, то при кибератаке на какой-нибудь военный объект американцы вправе будут ответить любым видом воздействия, в том числе и вооруженным. В то же время в киберпространстве очень сложно отследить всю цепочку атаки, с каких компьютеров был нанесен удар, особенно учитывая трансграничность. Поэтому задача обеспечения безопасного использования непрерывно развивающихся информационных технологий в условиях изменяющегося спектра угроз всегда остается актуальной.

Сложная международная обстановка и активизация террористических организаций усиливают угрозы информационной безопасности, 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, и для Союзного государства. Исходя из этого, одним из важных направлений работы является предупреждение и нейтрализация угроз информационной безопасности общих информационных ресурсов Республики Беларусь и Российской Федерации. С целью единого научно-технического обеспечения защиты общих информационных ресурсов двух стран непрерывно осуществляется работа по реализации программ по укреплению информационной безопасности государств – участников Союзного государства.

Белорусские и российские эксперты в области защиты информации подчеркивают, что стремительное развитие информационных и коммуникационных технологий и их активное внедрение во все сферы жизнедеятельности, а также формирование глобального информационного пространства выводят задачу по обеспечению информационной безопасности в разряд государственных приоритетов.

Уровень безопасности информационного пространства Союзного государства непосредственно влияет на возможность реализации прав и свобод граждан, на сохранение суверенитета и обеспечение стабильного развития экономики наших стран. При этом очевидно, что противодействие угрозам в информационной сфере возможно только на основе дальнейшего укрепления сотрудничества. В области защиты информации, противодействия киберпреступлениям Беларусь и Россия стараются идти вровень с самыми последними новациями, отслеживая современные тенденции развития компьютерных технологий, прилагая немало усилий, чтобы расширить компетенции специалистов в этой области, от которых во многом будет зависеть отражение угроз национальной безопасности в каждой из стран Союзного государства.

Снежана МИХАЙЛОВСКАЯ.
Фото Виктории КУКЛИНОЙ ■

