«Длинные руки» информационной безопасности

Ю.С. ХАРИН,
доктор физ.-мат. наук, директор Научно-исследовательского института прикладных проблем математики и информатики Белгосуниверситета

Возможность использования информационных и коммуникационных технологий (ИКТ) в неблаговидных целях становится фактором, оказывающим влияние на современные отношения в бизнесе и в обществе в целом. Каким представляется на сегодняшний день информационно-коммуникационное поле и какие у него наиболее уязвимые места? Какие проблемы инфобезопасности нуждаются в серьезной проработке?

Эти и ряд сопутствующих проблем мы попросили прокомментировать известного ученого, директора Научно-исследовательского института прикладных проблем математики и информатики Белгосуниверситета, член-корреспондента Национальной академии наук Беларуси, доктора физ.-мат. наук Юрия Семеновича ХАРИНА.

– Современное информационно-коммуникационное поле представляет собой глобальную информационную сферу – цифровой мир. Оно включает в себя также информационные пространства Республики Беларусь, корпоративные информационные пространства, становление и интенсивное расширение которых – неизбежная необходимость развития IT, имеющая необратимый характер. Объемы циркулирующей в них информации растут экспоненциально. Например, объем собираемых в США цифровых данных к 2020 г. превысит 7000 экзобайт (1 экзобайт = 10^{18} байт). Основные источники информации: интернет, социальные сети, мобильные устройства, данные с автоматических сенсоров, бизнес-информация. При этом именно информация является главным высокоценным ресурсом и товаром в цифровом мире, требующим защиты на всех этапах жизненного цикла. Сегодня это стало важнейшей проблемой национальной и международной безопасности.

Современный масштаб киберпреступлений впечатляет. Например, по данным компании IBM, ежегодные финансовые потери от киберпреступлений превышают 200 млрд долларов, причем ежесекундно в мире регистрируется 18 жертв киберпреступлений.

Практическое предотвращение утечек, обеспечение конфиденциальности, целостности и доступности информации предполагает несколько направлений защиты. Во-первых,

криптографическая защита информации (КЗИ); во-вторых – техническая защита, которая нацелена на недопущение несанкционированного доступа; защита от компьютерных вирусов и воздействий вредоносных программ. Третьим «заслоном» служат организационно-правовые методы.

Решением указанных проблем информационной безопасности занимаются сотни тысяч ученых и технических специалистов во всем мире.

– В сфере кибербезопасности давно известен бренд «Лаборатория Касперского». Существуют ли ли структуры подобного рода в Беларуси и какова их эффективность?

– В нашей республике, начиная с советских времен, весьма интенсивно развивались вычислительная техника и информатика. Потенциал IT-специалистов не только не был утерян, а наоборот, стал активно процветать под крылом «Инфопарка» и Парка высоких технологий. Подтверждением этой тенденции приоритетного развития IT-отрасли в стране является Декрет Президента Республики Беларусь № 8 «О развитии цифровой экономики».

В Беларуси существует мощная научная и практическая школа IT-технологий, поэтому можно говорить, что в республике давно и активно ведутся разработки компьютерных антивирусов. Основным разработчиком в этой области является созданная в 1997 г. компьютерная фирма ОДО «ВирусБлокАда» (резидент ПВТ), которая хорошо известна в стране и за рубежом своим антивирусным программным средством Vba32.

– Юрий Семенович, какие решения на сегодняшний день наиболее эффективны для защиты, например, банковских систем?

– На наш взгляд, эффективными для защиты банковских и других критически важных объектов являются такие решения, которые используют модель угроз информационной безопасности, методы гарантированной защиты от них и строгое организационно-правовое исполнение персоналом зафиксированных требований. Остановлюсь подробнее на рекомендациях и разработках нашей организации – учреждения Белорусского государственного университета «НИИ прикладных проблем математики и информатики» (НИИ ППМИ).

Криптографические методы в настоящее время являются основным способом защиты информации с гарантированной стойкостью и представляют собой систему криптографических алгоритмов и протоколов, а также инфраструктуру управления соответствующими ключами.

В 2007–2017 гг. в республике введена в действие разработанная в НИИ ППМИ серия стандартов в области криптографической защиты информации. Стандартизированы алгоритмы шифрования, имитозащиты, хеширования и управления ключами (СТБ 34.101.31, СТБ 34.101.77), разделения секрета (СТБ 34.101.60), генерации псевдослучайных чисел (СТБ 34.101.47), электронной цифровой подписи и транспорта ключа (СТБ 34.101.45), протокол TLS (СТБ 34.101.65), протоколы формирования общего ключа на основе эллиптических кривых (СТБ 34.101.66).

Стандартизированные алгоритмы и протоколы соответствуют лучшим зарубежным аналогам, а в некоторых случаях опережают их или не имеют таковых. Разработанные стандарты начинают широко применяться при построении республиканских систем защиты информации. Известные примеры – успешно работающая Государственная система управления открытыми ключами (ГосСУОК), набирающая обороты Межбанковская система идентификации (единое окно аутентификации для клиентов различных банков) и проектируемая инфраструктура Id-карт (идентификация, аутентификация и ЭЦП в духе Европейской инициативы eIDAS – Electronic IDentification, Authentication and trust Services).

Криптографические алгоритмы реализуются в программных или аппаратных средствах защиты. На сегодняшний день в стране создана разнообразная линейка таких средств, налажена система их сертификации. Сертификация СКЗИ опирается на еще один стандарт – СТБ 34.101.27. В стране имеются достаточно сильные компании, специализирующиеся на разработке криптографического ПО и аппаратуры.

Еще в 2013 г. в НИИ ППМИ разработаны и введены в действие 5 национальных стандартов специально для банковской сферы, при разработке которых решалась задача по поддержанию стабильности банковской системы Республики Беларусь в целом.

С принятием комплекта стандартов установлены единые требования безопасности для всех банков страны, процедуры оценки достаточности мер по обеспечению безопасности, методика оценки соответствия установленным требованиям. Это дает возможность Национальному банку на легитимной основе эффективно осуществлять контроль за обеспечением безопасности и защиты информационных ресурсов в банках и небанковских кредитно-финансовых организациях.

– Что, по вашему мнению, толкает людей на киберпреступления, что ими движет?

– Полагаю, что преступное желание незаконно завладеть информацией для повышения своего статуса в обществе (материального или морального). Думаю, что мотивы киберпреступлений мало чем отличаются от преступлений в другой сфере. Попутно хотелось бы отметить, что в профилактике киберпреступлений большое внимание необходимо уделять расширению осведомленности населения, начиная со школы, об информационной безопасности и информационном праве.

– Что нужно предпринимать компаниям, чтобы их сотрудники были начеку и не допускали утечек информации?

– Каждая компания должна иметь модель угроз информационной безопасности и эффективный способ ее защиты, о котором мы уже говорили. Но это еще не все. Как известно, самое слабое звено в любой системе защиты информации – это человек, сотрудник компании, поэтому все требования такой системы должны строго выполняться. Кроме того, надо помнить, что с течением времени стойкость любой системы защиты информации уменьшается (противник развивается!), поэтому необходима ее периодическая (хотя бы раз в 5 лет) контрольная аттестация.

– Какие, на ваш взгляд, направления в сфере кибербезопасности наиболее перспективны для изучения молодыми учеными?

– Как уже отмечалось, криптографический метод в настоящее время является основным методом защиты информации. Он базируется на новой науке – криптологии, объединяющей криптографию и криптоанализ. Среди перспективных, активно разрабатываемых в мировой науке следует выделить следующие направления криптологии:

построение криптографических алгоритмов и протоколов с гарантированной стойкостью;

разработка стойких криптографических генераторов случайных и псевдослучайных последовательностей;

оценка информационной безопасности технологии блокчейн и криптовалют;

квантовая криптография и целый ряд других.

– Представьте, пожалуйста, вкратце ваш институт. Какие основные задачи стоят сейчас перед ним, каковы главные направления работы?

Учреждение Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики» (сайт http://apmi.bsu.by) создано в 2000 г. специальным Постановлением Совета Министров Республики Беларусь «в целях развития и координации в Республике Беларусь теоретических и прикладных научных исследований в области криптографической защиты информации, компьютерного моделирования и анализа данных». В институте работают свыше 60 научных сотрудников (штатных и совместителей), в т. ч. 8 докторов наук и 33 кандидата наук; к выполнению НИОКР привлекаются аспиранты, магистранты и студенты.

Главные направления научной работы НИИ ППМИ в настоящее время: теоретические и прикладные исследования в области защиты информации для электронного документооборота страны; проведение экспертизы и сертификационных испытаний средств криптографической защиты информации; теоретические и прикладные исследования в области компьютерного анализа данных (Data Science).

Беседу вела Алиса РОМАНОВИЧ,
«Веснік сувязі»