Научно-технический прогресс движется вперед семимильными шагами, принося цивилизации все новые блага. Но одновременно с ними возникают и проблемы.

Например, информатизация, ставшая неотъемлемой частью общества. Она порождает риск зависимости каждого своего субъекта (государства, общества или человека) от глобального информационного пространства, риски информационных войн, информационного шпионажа и т.д. Поэтому обеспечение информационной безопасности – одна из приоритетных задач развитых стран.

О проблемах информационной безопасности рассказывает зав кафедрой теоретической кибернетики ИВМиИТ КФУ, член-корреспондент АН РТ, профессор ***Фарид Аблаев****:*

– Фарид Мансурович, начнем с того, что такое информационная безопасность, и как её обеспечить?

– Информационная безопасность – это сохранность информационных ресурсов и защищенность законных прав личности и общества в

информационной сфере. В ней можно выделить 3 составляющие: конфиденциальность, целостность и доступность информации. Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям; целостность – обеспечение достоверности и полноты информации и методов ее обработки; доступность – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и/или на другие ресурсы автоматизированной информационной системы. При этом, ее обеспечение – дорогое дело – из-за затрат на закупку и установку средств защиты, а также из-за необходимости поддержания системы в работоспособном состоянии.

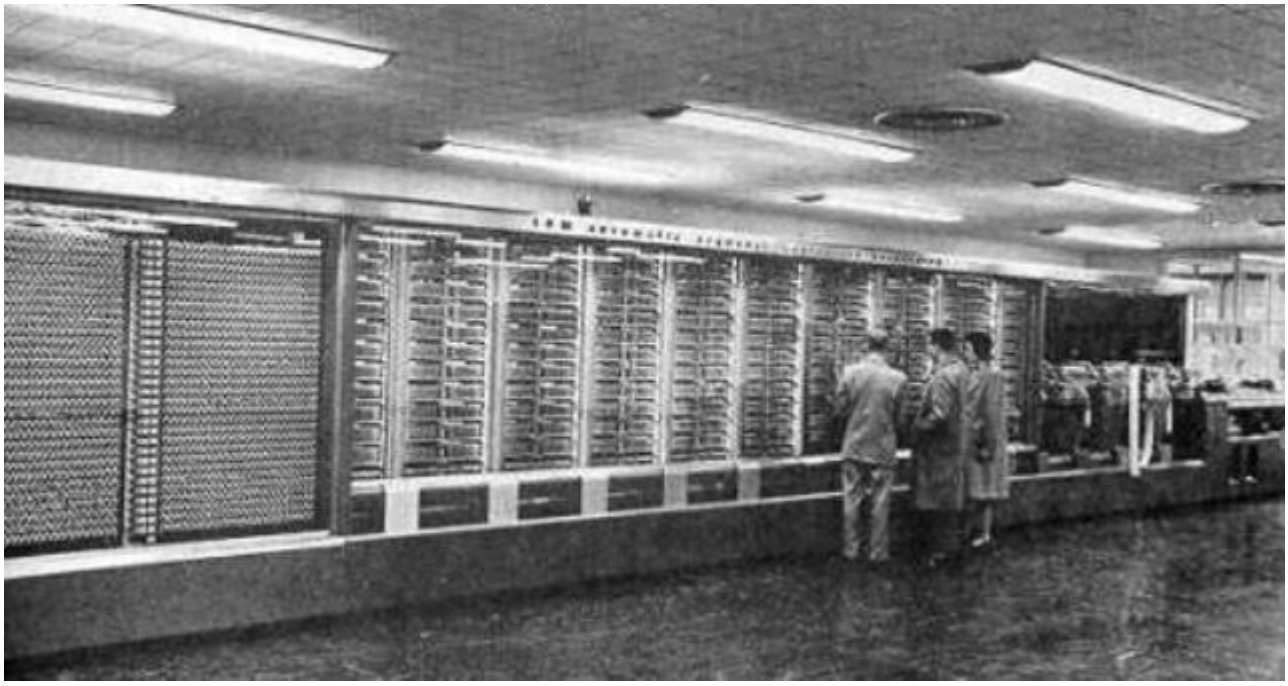
Вообще, информационная безопасность – один из древнейших видов деятельности. Люди всегда шифровали письменные тексты, содержание которых должны были знать только адресаты. Ведь если отправить с гонцом незашифрованный текст, то узнать его содержание было нетрудно – гонца можно было напоить или просто ограбить. В случае шифрования это становилось бесполезным.

Кстати, древнейший из известных нам шифров называют «Шифром Цезаря», что прямо указывает на эпоху его применения. Он основан на «сдвиге», когда каждый символ исходного текста заменяется символом, который находится в алфавите на некотором постоянном числе позиций левее или правее него. Например, в шифре со сдвигом вправо на 3 символа вместо «А» ставится «Г», «Б» заменяется на «Д» и так далее.

Одна из схем «Шифра Цезаря»

В те давние времена, когда по-настоящему грамотных людей было очень мало, расшифровка такого текста становилась почти невозможной. Но сейчас, конечно, она не представляет затруднений: есть статистика количества и повторения тех или иных букв в тексте, есть таблицы наиболее часто встречающихся букв для разных языков. Поэтому опытный лингвист не сочтет «Шифр Цезаря» сложной задачей.

Но шифры разной степени сложности успешно применялись вплоть до широкого распространения вычислительной техники, которое сделало вопросы информационной безопасности особенно актуальными. Например, стала острее проблема идентификации – а с нужным ли адресатом было установлено сообщение? Еще один пример – электронная цифровая подпись, которой сейчас пользуются очень многие. Ее вариант – разные PIN-коды, например, в банковских картах.



Первый в мире компьютер «Mark I»

А для армии и других силовых структур понадобились системы распознавания «Свой – чужой». Например, противовоздушная оборона – система опознания запрашивает неизвестный самолет о его принадлежности с помощью шифрованного сигнала. С самолета должен прийти ответный сигнал, подтверждающий: «Я – свой». Если его нет, можно поднимать в воздух истребители-перехватчики или запустить зенитную ракету.

Что касается обеспечения информационной безопасности – она достигается целым комплексом мер. Во-первых, технологические, воздействующие на каналы связи. Во-вторых, сами алгоритмы шифрования – оказалось, что секретом должны быть не они сами. Как выяснилось, здесь наиболее эффективны математические способы, например, использование односторонних функций. Они легко вычисляются по заданным аргументам, а вот в обратную сторону – восстановить аргумент такой функции по ее значению крайне сложно.

Кстати, это было осуществлено еще до наступления компьютеризации. Вспомните семейство электромеханических роторных шифровальных машин **«Enigma«** (от др.-греч. αἴνιγμα – «загадка»), разработанную в Германии в 20-х годах прошлого

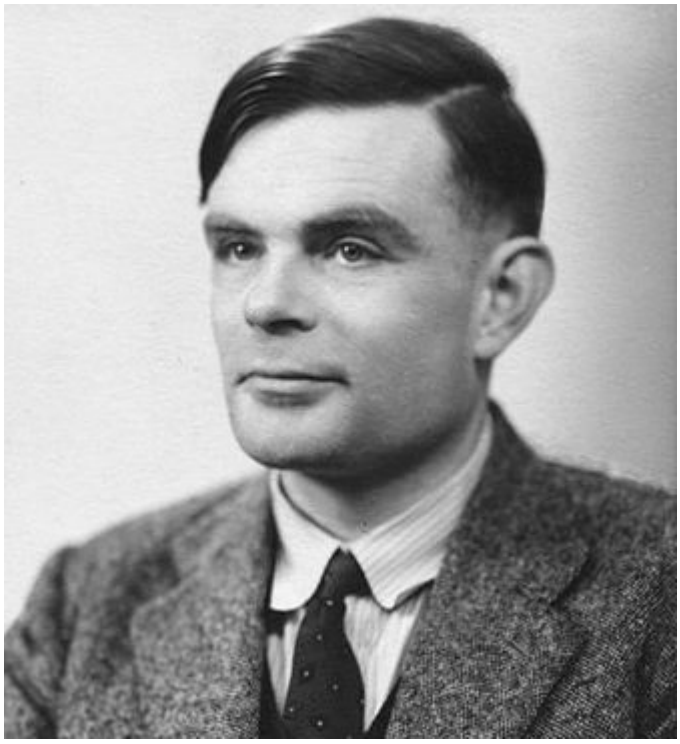
века. Ее работа была совершеннейшим вариантом «Шифра Цезаря» со сложнейшими, постоянно чередующимися сдвигами. Но оказалось, что и ее хитрости можно разгадать.

Один из вариантов машины «Enigma»

Впервые это сделали в конце 1932 г. польские ученые-математики (а по совместительству – разведчики) Мариан Реевский, Ежи Рожицкий и Генрих Зыгальский – по полученным от французской разведки данным, с помощью математической теории и методов обратной разработки. Польские специалисты создали «Криптологическую бомбу» – специальное устройство для расшифровки закодированных «Энигмой» сообщений. После этого немецкие инженеры усложнили устройство своей машины.

2-й раз «Энигму» разгадали во время II Мировой войны. Это осуществила группа математиков, работавшая в Правительственной школе кодов и шифров Великобритании. Одну из групп этой школы – Hut 8 (занимавшуюся расшифровкой сообщений кригсмарине –

военно-морского флота Германии) – возглавлял английский математик, логик и криптограф Алан Тьюринг, создавший в 1936 г. абстрактную вычислительную машину («Машина Тьюринга») для формализации понятия «алгоритм». То и другое стало основанием для современной информатики, в частности, для теории искусственного интеллекта. Тьюринг использовал свои разработки для создания методов взлома немецких шифров. В их числе была теоретическая база для «Bombe» – машины, распутавшей хитросплетения «Энигмы».



Алан Тьюринг

– А какими компетенциями должен обладать специалист по информационной безопасности?

– В идеале он должен быть хорошо подкован в области специальной дискретной математики и конечной алгебры, а также в программировании – особенно, в построении быстрых алгоритмов (это алгоритмы вычисления заданной функции с заданной точностью с использованием как можно меньшего числа битовых операций). Очень желательно, чтобы он знал устройство «железа» и принципы его работы, соответственно, ему нужны знания в области радиоэлектронных технологий, а это уже физика. Кроме

того, атака электронной информационной системы может быть направлена на питающую ее электросеть, что может повлиять на процесс шифрования. Поэтому шифровальные программы могут работать изолированно от сети – они получают энергию от встроенных аккумуляторов. Специалист должен во всем этом хорошо разбираться!

Наконец, такой профессионал должен обладать определенным объемом знаний в области психологии и юриспруденции. По поводу психологии: известно, что, если предложить системному администратору пятикратно превышающее его годовую зарплату разовое вознаграждение, то перед такой перспективой мало кто устоит. Поэтому, кстати, современные шифровальные системы не связаны с людьми: в них используются датчики случайных символов. Это так называемые программы-роботы, которые создают используемую при шифровании информацию, доступа к которой нет ни у кого. Ну, а юриспруденция – знание законов об авторском праве и защите информации, тем более, что они сейчас постоянно модернизируются.

Но вернемся к математике: в современном шифровании очень большое значение имеет теория чисел – оказалось, что здесь имеют важное значение так называемые эллиптические функции – заданные на комплексной плоскости аналоги тригонометрических, имеющих только один период. Сегодня шифрование с их использованием – общепринятый стандарт. Вот так фундаментальная математика стала прикладным средством шифрования!

– Одним словом, профессия специалиста по обеспечению информационной безопасности в будущем станет одной из наиболее востребованных?

– Без всякого сомнения, ведь абсолютно все сферы жизни современного общества стремительно информатизируются, причем, этот процесс происходит даже на периферии мировой цивилизации. Более того, сейчас активно идут разработки принципиально новой вычислительной техники – квантовой. Обеспечение информационной

безопасности понадобится и там, при этом, оно должно основываться на совершенно других принципах. Кстати, имеющиеся сейчас квантовые компьютеры, несмотря на их невысокую (пока!) мощность, уже достаточно хороши в качестве криптографических устройств и применяются именно для этого – тех кубитов, которыми они располагают, мало для проведения сложных вычислений, но достаточно для эффективной криптографии. Выпускаются и квантовые датчики случайных символов, получающие все более широкое распространение.

Квантовый компьютер «D-Wave»

Используется в криптографии и такое свойство известных квантовых частиц: ни одну из них нельзя копировать. Ведь как осуществляется традиционная дешифровка информации? Обычно перехватывается какой-то ее объем, затем он сохраняется и анализируется. А вот квантовые технологии делать это не позволяют: если мы хотя бы раз извлекли из частицы информацию, то мы ее, грубо говоря, погубили – больше эту частицу использовать невозможно.

– В ИВМиИТ КФУ действует магистерская программа «Математические методы и программные технологии защиты информации». Думаю, читателям – потенциальным студентам было

бы интересно узнать, какие возможности открывает обучение по ней?

– Обучение по этой магистерской программе осуществляется только на контрактной основе, преподаватели – ученые ИВМиИТ и Института физики. Мы готовы набирать группы математиков и физиков и вести их совместную подготовку. Она, в свою очередь будет междисциплинарной – там есть дискретная математика, теоретическая и квантовая физика, радиоэлектроника. Кстати, в зарубежных вузах и научных центрах такое давно практикуется – там есть специалисты, хорошо подготовленные в дискретной математике, в теоретической и квантовой физике. У нас пока в этой сфере – кадровый дефицит. Именно такой комплекс научных дисциплин, востребованный и эффективный, мы сейчас и создаем.

Окончившие эту магистратуру будут по-настоящему уникальными профессионалами. Они будут востребованы во всех сферах жизни государства и общества, где нужна деятельность, связанная с хранением, обработкой и передачей больших массивов информации, а также с ее защитой: бизнес, СМИ, банковское дело, медицина, образование, различные сферы государственной службы – дипломатия, армия, органы охраны правопорядка и т.д. Так что проблем с трудоустройством у выпускников магистратуры точно не будет!

– Фарид Мансурович, молодежь сейчас повально увлечена различными гаджетами – игры и соцсети стали чуть ли не главным смыслом ее жизни. Поможет ли это молодым людям в полной мере овладеть IT-наукой, в том числе и информационной безопасностью?

– Если заниматься только компьютерными играми и общением в соцсетях – то вряд ли. А вот если человек заинтересуется, как это все работает, и начнет выискивать нужную информацию в том же интернете – то да, такой подход к делу безусловно поможет. Но это будет только первый шаг – овладеть специальными знаниями IT-науки можно лишь в вузе. Причем, делать это нужно ступенчато – например, на уровне бакалавриата надо готовить универсальных специалистов: сразу углубляться в узкоспециализированные области не стоит.

Подготовка бакалавров тоже должна разделяться на этапы: общая подготовка по физике и математике, затем по IT-технологиям, а на уровне дипломной работы – уже специализация. Следующий этап – магистратура. К моменту поступления в нее студент уже должен определиться, что конкретно его интересует, и заниматься

именно этим. Будет очень хорошо, если в магистратуру поступает человек, уже имеющий опыт работы – как правило, такие уже точно знают свои возможности, а также то, чего они хотят.

– А какие технологии защиты информации разрабатываются в КФУ?

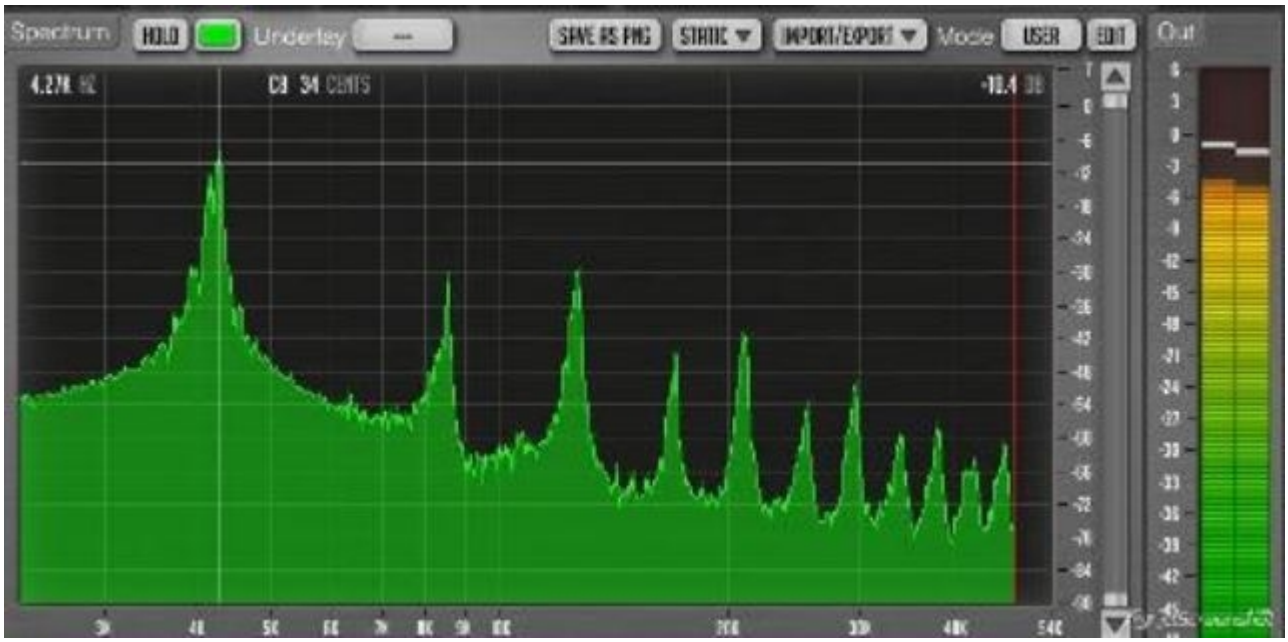
– Во-первых, на кафедре радиофизики Института физики над системами защиты каналов связи работает научная группа под руководством завкафедрой, профессора **Олега Шерстюкова** (***прим. авт.:*** *об этой работе «Казанский университет» писал 20 октября прошлого года*). У них готово уже немало технологических разработок и предложений. У нас в ИВМиИТ есть 2 научные группы, занимающиеся вопросами защиты информации. Одна работает над классической криптографией в рамках специальной теории чисел, а другая, в которую вхожу и я – над системой квантовой криптографии.

В рамках этих исследований мы тесно взаимодействуем с Академией криптографии РФ – совместно с ней в прошлом году провели в Казани при активном участии МИАН (Математического института им. В.А.Стеклова РАН) IV симпозиум **«Современные тенденции в криптографии»**, посвященный математическим и техническим проблемам отечественной криптографии и защиты информации. На этом научном форуме лидирующие разработчики систем информационной безопасности формируют основные направления развития данной отрасли в России.

Напоследок такой вопрос: исследование Telesign обнаружило – 69% профессионалов в области безопасности считают, что пароли и пользовательские имена не являются достаточной защитой для компаний, а 72% уверены, что их перестанут использовать в течение следующих 10 лет. На их место придут альтернативы, такие как поведенческая биометрика и двухфакторная аутентификация. Это поможет спастись компаниям от атак мошенников?

– Совершенно верно. На сегодняшний день система аутентификации такая: логин и пароль. Понятно, что на нее идут постоянные

атаки и ее эффективность недостаточна. Соответственно, нужно переходить к новым, более сложным уровням, той же двухфакторной аутентификации (2FA), при которой для входа в систему нужны не только логин и пароль, но и что-то еще, например, персональный идентификационный номер (PIN-код), номер телефона или биометрические параметры: отпечатки пальцев или voice print – идентификация по «отпечатку» (контурной спектрограмме) голоса. Поведенческая биометрика, как система распознавания людей по физическим или поведенческим чертам, также может найти применение в IT-технологиях защиты информации.



Спектрограмма человеческого голоса

– Словом, все сканирующие радужную оболочку глаз или голос «секретные замки», столь любимые создателями фантастических фильмов – дело недалекого будущего?

– Это уже дело настоящего. А в недалеком будущем они перестанут быть атрибутом чего-то жутко секретного и получат массовое распространение.

Фото Алсу Гараповой и из архива редакции.