Российский государственный гуманитарный университет
Russian State University for the Humanities

RSUH/RGGU BULLETIN

№ 14 (94)

Academic Journal

Series
Computer Science. Data Protection. Mathematics

Moscow 2012

В Е С Т Н И К Р Г Г У

№ 14 (94)

Научный журнал

Серия «Информатика. Защита информации.
Математика»

Москва 2012

УДК 94 (560)
ББК 63.3(5)я5

ISSN 1998-6769

СОДЕРЖАНИЕ

Проектирование

CONTENTS

Design

ОТ РЕДАКЦИИ

Предлагаем вашему вниманию очередное издание серии «Информатика. Защита информации. Математика» журнала «Вестник РГГУ», в котором продолжается обсуждение таких актуальных вопросов, как анализ угроз информационной безопасности, проектирование систем защиты, семантические аспекты информатики, функциональная устойчивость информационных систем и др.

В разделе «Тема номера» помещены статьи, посвященные электронному документообороту. В связи с увеличением числа организаций, внедряющих современные технологии для улучшения документооборота, рассматриваемые вопросы в данной области становятся особо актуальными. Следует также отметить проблемы информационной безопасности, связанные с распространением облачных вычислений. Под термином «облачные технологии» понимают набор программных и аппаратных технологий, обеспечивающих пользователя клиент-серверных приложений повышенной надежностью, производительностью, новыми возможностями. Несмотря на преимущества подобной инфраструктуры, возникает ряд задач, требующих исследования, например оценка отказоустойчивости, передача информации по каналам связи, виртуализация.

Приглашаем авторов – преподавателей РГГУ и его филиалов, сотрудников научных центров, представителей большого и малого бизнеса, аспирантов, докторантов – к публикации результатов научных исследований по современной проблематике информационных технологий и математики.

Материалы для журнала просим оформлять в соответствии с принятыми нормами, установленными ВАК для рецензируемых научных изданий, и направлять их электронной почтой по адресу: vestnik@rggu.ru на имя ответственного редактора серии А.А. Тарасова.

Д.А. Ларин

ЗАЩИТА ИНФОРМАЦИИ И КРИПТОАНАЛИЗ В СССР ВО ВРЕМЯ СТАЛИНГРАДСКОЙ БИТВЫ

17 июля 2012 исполнилось 70 лет с начала одного из крупнейших сражений в истории войн – Сталинградской битвы. Это сражение, закончившееся полным разгромом группировки немецко-фашистских войск и их союзников, стало переломным моментом Второй мировой войны. Важная роль в победе под Сталинградом принадлежит советским криптографам. Разработчики шифров и шифрмашин, шифровальная служба и войска связи обеспечили безопасность советских линий связи. Радиоразведчики и дешифровальщики успешно перехватывали и дешифровывали криптограммы фашистской Германии и ее европейских союзников.

Ключевые слова: криптография, шифрование, дешифрование, шифр, шифратор, связь, Сталинград.

К лету 1942 г. немцы оправились после поражения под Москвой, началось наступление на южном направлении. В летне-осенней кампании 1942 г. войскам вермахта вновь удалось овладеть стратегической инициативой и продвинуться к Воронежу, Волге и предгорьям Кавказа. Советским командованием был создан Воронежский фронт. В населенном пункте Поворино были развернуты работы по монтажу узлов и организации связи. Немцы бомбили Поворино ежедневно, во время каждой бомбежки связисты и криптографы скрывались в ближайшем овраге, а потом вновь продолжали работы. Вот что вспоминает один из офицеров-связистов П.Н. Воронин: «Однажды, вернувшись из укрытия, увидели догорающие обломки зданий, где мы разместили наши узлы. Погибло и все оборудование. Нашлись “когти” и телефонный аппарат.

Влезли на столб с сохранившимися проводами. А.А. Конюхов и я доложили своим руководителям о случившемся. Но к этому времени обстановка изменилась, и ВЧ-связь развернули в деревне Отрадное, куда вскоре переместился и штаб фронта. Вскоре мне было приказано срочно выехать в Сталинград»[1].

Именно этот город стал главной целью фашистских захватчиков. Падение Сталинграда привело бы к потере последних коммуникаций, связывающих центральные районы СССР с Кавказом, где проходили главные артерии страны по транспортировке бакинской нефти. Это обстоятельство предопределило ход боевых действий. Успешные боевые действия требуют организации надежной связи, во время Сталинградской битвы советские связисты предпринимали героические усилия по подержанию функционирования сетей связи с оборонявшейся на правом берегу Волги группировкой советских войск. Задача эта была крайне непростой. По просьбе командования фронтов и в соответствии с решениями Ставки ВГК Отдел правительственной связи (ОПС) НКВД путем мобилизации всех имевшихся сил и средств к середине октября 1942 г. обеспечил организацию правительственной связи в звене фронт–армия с учреждением ВЧ-станций при штабе каждой армии. В кратчайшие сроки было развернуто до 60 армейских станций и около 20 армейских узлов связи[2]. В течение 1941 и первой половины 1942 г. было создано 9 новых крупных узлов правительственной связи, из которых 5 предназначались и использовались специально для функционирования высокочастотной телефонной (ВЧ) связи Ставки ВГК с конкретными фронтами, кроме того для связи со Сталинградским фронтом использовались Куйбышевский и Саратовский узлы связи. Эти узлы стали центрами локальных сетей, объединявших десятки станций и усилительных пунктов правительственной связи. Например, схема ВЧ-связи Куйбышевского узла включала около 30 станций и трансляционных пунктов. Роль усилительных пунктов на этих сетях была достаточно велика. Так, через Ряжский транспункт проходили уплотненные ВЧ-каналами цепи таких важнейших направлений, как Москва–Сталинград, Москва–Куйбышев (ныне Самара), Москва–Воронеж и Москва–Хабаровск. Выход из строя этого пункта повлек бы за собой тяжкие последствия. Поэтому руководством центральных и периферийных органов ОПС так много внимания уделялось обеспечению живучести тыловых узлов. Усилившиеся авианалеты немцев на города, в которых располагались основные узлы правительственной связи, вызвали необходимость

срочной организации в ряде населенных пунктов резервных станций. Такие станции были построены в 15 городах, в том числе и в Сталинграде. В случае выхода из строя основной станции была предусмотрена возможность немедленного переключения всех связей на резервную станцию[3].

Организация проводной (в том числе высокочастотной телефонной) связи во время Сталинградского сражения затруднялась тем, что в полосе действия Сталинградского фронта сеть постоянных воздушных линий (в которых провода навешаны на телеграфные столбы) была развита недостаточно. Имевшиеся линии обеспечивали телеграфно-телефонную связь только в пределах Сталинградской области и по своему количеству и качеству не могли удовлетворить всех потребностей фронта в период активных боевых действий в районе Сталинграда. Местные линии, проходившие по территории, на которой шли боевые действия, имели технические недостатки, затруднявшие дополнительную подвеску проводов; большинство из них требовало ремонта. К тому же местные линии в своей основной части не совпадали с оперативными направлениями. По этим причинам с началом боевых действий на дальних подступах к Сталинграду потребовалось строительство новых линий для обеспечения связи Ставки ВГК со штабами фронтов и штабов фронтов с армиями.

Войска связи Сталинградского фронта совместно со строительными организациями Народного комиссариата связи (НКС) только в период с июля по декабрь 1942 г. построили около 400 км новых линий связи и подвесили около 2000 км проводов. Строительство новых линий было крайне затруднено тем, что запас телеграфных столбов и проволоки на складах был недостаточен, а подвоз их, ввиду перегрузки транспорта, крайне ограничен. Заготовка телеграфных столбов на месте почти полностью исключалась вследствие отсутствия в районе боевых действий лесных массивов.

Среди мероприятий по организации четкого функционирования ВЧ-связи в оборонительной и наступательной операциях Сталинградской битвы выделялись, в частности, подвеска и приведение в нормальное техническое состояние медной цепи на магистральной линии Урбах–Эльтон–Харабали–Астрахань. Для обеспечения обходной связи Ставки ВГК со штабом Сталинградского фронта была построена постоянная воздушная линия от Сталинграда через Ново-Казанку до Урала. Кроме того, при подходе немецко-фашистских войск к Сталинграду ВЧ-станция Сталинградского УНКВД была разделена на две: одна предназначалась

для обслуживания штаба Сталинградского фронта (начальник фронтового ОПС А.Д. Кураков), ее возглавил начальник отделения ПС Сталинградского УНКВД А.Н. Панченко; другая – для обеспечения связи штаба 62-й армии со штабом фронта, она работала под руководством В.Е. Овчарова.

В Сталинграде сложилась очень тяжелая обстановка. Все основные линии связи Москвы со Сталинградом шли по правому берегу Волги. После того как немцы вышли на ее берег выше Сталинграда, в местечке Рынок, и ниже Сталинграда, в районе Красноармейска, город оказался в окружении, после чего линии связи на правом берегу была оборвана.

Обслуживание линий ВЧ-связи во время боев под Сталинградом происходило в тяжелейших условиях. Восстановительными группами отдельных линейно-эксплуатационных рот ОПС НКВД практически непрерывно велись работы по ликвидации последствий бомбардировок. Например, на участке 924-й отдельной линейно-эксплуатационной роты связи (ОЛЭРС), обслуживавшей линию ВЧ-связи на подступах к Сталинграду, в некоторые дни связь нарушалась более 70 раз. Особенно тяжело было обеспечить связь со штабом 62-й армии, находившимся в самом городе. Связисты непрерывно прокладывали кабельные линии через Волгу, но они часто нарушались артиллерийским и минометным огнем, повреждались проходившими судами и баржами. К тому же кабели были полевого типа: промокая, они теряли изоляцию, и связь нарушалась. Такие кабели могли служить не более 3 суток, и в сложнейших условиях приходилось прокладывать новые. Так, с 11 по 13 ноября не работали все кабели, по которым штаб Сталинградского фронта поддерживал связь со всеми входившими в него армиями.

23 августа 1942 г. немцы произвели массированный авиационный налет на Сталинград. Весь город горел. В ходе оборонительных боев сама ВЧ-станция штаба Сталинградского фронта оказалась под угрозой захвата противником. Связисты НКС в тяжелейших условиях вывезли все оборудование междугородной станции на левый берег Волги и смонтировали резервный узел в местечке Капустин Яр с выходом на Астрахань и Саратов.

В Сталинграде действующих линий связи не осталось. Штаб Сталинградского фронта был на правом берегу. Связь с ним можно было организовать только с левого берега. Вторая ВЧ-станция Сталинграда также была вывезена на левый берег в местечко Красная слобода. Было получено указание тянуть проводную линию

через Волгу. Для координации действий фронтовых и территориальных органов, а также линейных подразделений правительственной связи в ходе Сталинградской оборонительной операции в Сталинград прибыл заместитель начальника ОПС НКВД П.Н. Воронин. При его непосредственном участии, в частности, был проложен подводный речной кабель через Волгу. Позже он вспоминал, что в первую очередь проверили, нельзя ли использовать имеющийся кабельный переход в районе захваченного немцами Рынка. Выяснилось, что подъехать к кабельной будке было сложно – немцы контролировали все подходы. И все же наши связисты добрались до нее и проверили исправность кабеля. Он работал, но на другом конце отвечали немцы. Использовать этот кабель было нельзя. Оставался один выход – прокладывать новый кабельный переход через Волгу. Ввиду отсутствия речного кабеля было принято решение класть полевой кабель ПТФ-7, не приспособленный для работы под водой, так как он промокал через 1–2 суток. Позвонили в Москву, чтобы срочно прислали речной кабель. Прокладку приходилось вести под непрерывным минометным обстрелом. Большой вред наносили плывущие по реке нефтеналивные баржи. Пробитые снарядами, они плыли по течению, постепенно погружаясь в воду, и перерезали кабели. Каждый день приходилось класть все новые и новые пучки кабельных линий на правом берегу Волги. Коммутатор ВЧ-связи был установлен в блиндаже, где размещалось командование фронта. На этот коммутатор связь по проводам передавалась с ВЧ-станции, находящейся на левом берегу. Наконец был доставлен речной кабель, барабан с которым весил больше тонны. Подходящей лодки для его перевозки и установки не нашлось, поэтому для этой цели был изготовлен специальный плот. Когда ночью началась прокладка кабеля, немцы засекли проведение работ и минометным огнем разбили плот. Пришлось начинать все сначала. Немецкие минометчики обстреливали советских связистов не один раз, гибли люди и плоты. Но в конце концов работу удалось завершить, и наконец кабель был проложен. До ледостава он работал надежно, но после того как Волга замерзла, в дополнение к подводному кабелю ВЧ-связь была организована по воздушной линии на столбах, вмороженных в лед, а также по проложенному по льду кабелю.

Если стационарные подразделения в период Сталинградского сражения были практически полностью укомплектованы личным составом и оснащены необходимым оборудованием, то организационная структура, численность и техническая оснащенность

отдельных линейно-эксплуатационных рот связи, составлявших основу линейной службы ОПС НКВД, еще не отвечали требованиям, которые выдвигались переходом советских войск к наступательным операциям. Так, во время Сталинградской битвы количество сил и средств линейной службы ОПС НКВД в полосе действий фронтов, задействованных в грандиозном сражении, явно не соответствовало объему поставленной перед связистами задачи. По состоянию на 31.12.1942 г. работы по эксплуатации линий ВЧ-связи выполнялись: в полосе действий Воронежского фронта (начальник ОПС П.П. Изотов) только силами 935, 941 и 749 ОЛЭРС, Юго-Западного (М.В. Катков) – 928 ОЛЭРС, Донского (А.Д. Кураков) – 751 ОЛЭРС, Сталинградского (А.Н. Панченко) – 924 и 931 ОЛЭРС. Однако несмотря на трудности, надежная связь в течение всего сражения была обеспечена. В феврале 1943 г. Сталинградская битва завершилась разгромом немецких войск. Связь со Сталинградом стала работать по довоенной схеме[4].

Само наличие линий связи не гарантирует надежное управление войсками. Необходимо обеспечить секретность передаваемой по каналам связи информации. Для этого применяются криптографические методы защиты информации. Советские войска во время Сталинградской битвы использовали различные коды и шифры, которые обеспечивали надежное шифрование военной и политической информации. Однако, как отмечалось выше, с организацией проводной связи в районе боевых действий были определенные трудности, которые приводили к необходимости использования радиосвязи. При этом следует отметить, что процессы шифрования и расшифрования в то время в большинстве случаев выполнялись вручную и занимали значительное время, а его в условиях быстро меняющейся оперативной обстановки часто не было. Идеальным выходом было применение для управления войсками голосовой (радиотелефонной и проводной ВЧ-связи), однако имевшиеся в то время на вооружении наших войск аппараты шифрования речевого сигнала не обладали достаточной криптостойкостью и не могли быть использованы для защиты информации стратегического характера. Решение данной проблемы предложил выдающийся советский ученый, впоследствии академик В.А. Котельников[5]. Еще в 1938–1939 гг. в ЦНИИ связи Наркомата почт и телеграфа (НКПиТ) были организованы две лаборатории под его руководством по засекречиванию телеграфной и телефонной информации. В.А. Котельников впервые в СССР разработал принципы построения телеграфной засекречивающей

аппаратуры, реализованные в аппаратуре «Москва», которые заключались в наложении на знаки телеграфного сообщения знаков шифра (гаммирование). В 1939 г. В.А. Котельникову было поручено решение важной государственной задачи – создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию. Заказчиком аппаратуры был отдел правительственной ВЧ-связи. Помимо В.А. Котельникова, участие в работах по секретной телефонии принимали А.Л. Минц, К.П. Егоров, В.К. Виторский и многие другие специалисты. Разработка шифратора имела оборонное значение, и для ее завершения лаборатория, входившая в состав Государственного союзного производственно-экспериментального института (ГСПЭИ № 56 НКЭП), осенью 1941 г. была эвакуирована в Уфу, где ее сотрудники объединились с группой специалистов, занимавшихся подобной разработкой на заводе «Красная заря» в Ленинграде. Институт возглавил К.П. Егоров, а в 1943 г. В.А. Котельников. Институт разработал каналообразующую аппаратуру СМТ-42 («Сойка») и ТВЧ-42 («Стриж»). Лаборатория В.А. Котельникова была разделена на две части: основная часть вместе с руководителем была эвакуирована в ГСПЭИ № 56, а другая часть была передана в НКВД СССР. В специальной лаборатории Центрального научно-исследовательского института связи была предложена система, основанная на квазислучайных (известных только получателю) перестановках временных (100 миллисекунд) отрезков речи и двух частотных полос с инверсией речевого сигнала. Управление частотными и временными перестановками на передаче и приеме осуществлялось специальным шифратором. Аппаратура была создана к осени 1942 г. и получила название «С-1» («Соболь»)[6].

Несмотря на все трудности военного времени, уже к осени 1942 г. сотрудники лаборатории Котельникова изготовили несколько образцов оборудования для секретной КВ-радиотелефонии под индексом «Соболь-П». Это была самая сложная из разрабатываемых в стране аппаратура засекречивания передаваемой информации, не имевшая аналогов в мире. Первые аппараты сразу направили под Сталинград для связи Ставки Верховного главнокомандования со штабом Закавказского фронта, проводная связь между которыми была нарушена во время боев. В то время в армии для связи такого уровня пользовались в основном проводными телефонными линиями, а «Соболь-П» позволил устанавливать связь посредством радиоканала. Это сыграло положительную роль в улучшении управления войсками, участвующими в Сталинградской битве.

К началу 1943 г. было налажено производство усовершенствованной серии аппаратов «Соболь-П». Сложные механические узлы уникальных шифраторов, разработанных в лаборатории Котельникова, изготавливались на одном из ленинградских заводов. Для окончательной наладки шифраторов Котельников регулярно летал в блокадный Ленинград, при этом не раз попадал под обстрелы и бомбардировки. Готовые аппараты срочно отправляли на фронт. Как вспоминали ветераны Великой Отечественной войны, применение шифраторов Котельникова в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы. Они обеспечивали шифрование речи при передаче по радио. Шифраторы практически не поддавались взлому, это оказалось не по зубам даже лучшим немецким дешифровальщикам. По сведениям советской разведки, Гитлер заявлял, что за одного криптоаналитика, способного ее «взломать», он не пожалел бы три отборные дивизии.

За создание шифраторов В.А. Котельников и его коллеги по лаборатории (И.С. Нейман, Д.П. Горелов, А.М. Трахтман, Н.Н. Найденов) получили в марте 1943 г. Сталинские премии I степени. Деньги они передали «на нужды фронта». В частности, на премию, полученную В.А. Котельниковым, был построен танк. В дальнейшем аппаратура «Соболь-П» активно использовалась для связи Ставки Верховного главнокомандования с фронтами. После окончания Второй мировой войны она получила применение и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций глав трех государств и для связи с Москвой нашей делегации во время принятия капитуляции Германии в мае 1945 г. Работа над усовершенствованием шифровальной аппаратуры продолжалась до последних дней войны и даже после ее окончания. За дальнейшие разработки в этой области группе специалистов и В.А. Котельникову в 1946 г. была присуждена вторая Сталинская премия I степени[7].

При этом следует отметить, что, несмотря на наличие современных средств шифрования, советские военачальники во время Великой Отечественной войны нередко отказывались от передачи важной информации по сетям связи. Так, во время подготовки контрнаступления под Сталинградом в 1942 г. советское военное руководство особое внимание уделяло скрытности подготовки контрудара: «Переписка и телефонные разговоры, связанные

с предстоящим контрнаступлением, были категорически запрещены; распоряжения отдавались в устной форме и только непосредственным исполнителям; сосредоточение и перегруппировка войск проводились только ночью. Ставка незамедлительно и резко реагировала на любое нарушение скрытности подготовки контрнаступления»[8]. В частности, была издана директива, адресованная командующему Сталинградским фронтом, в которой говорилось: «Ставка Верховного главнокомандования категорически запрещает Вам впредь пересылать шифром какие бы то ни было соображения по плану операции, издавать и рассылать приказы по предстоящим действиям. Все планы операции по требованию Ставки направлять лишь только написанными от руки и с ответственным исполнителем. Приказы на предстоящую операцию командующим армиями давать только лично по карте»[9]. Сохранению секретности всех вопросов, касавшихся проведения контрнаступления, «способствовало также пребывание на фронтах представителей Ставки ВГК Г.К. Жукова и А.М. Василевского. Они решали на местах, без переписки между генштабом и командованием фронтов, не только вопросы организации взаимодействия между фронтами, но и другие принципиальные вопросы планирования и подготовки операции»[10].

Обеспечение скрытности подготовки контрнаступления было одной из главных задач, ставившихся всем соединениям, участвовавшим в операции. В качестве примера рассмотрим 5-ю танковую армию. «С планом операции был ознакомлен лишь узкий круг офицеров и генералов, и только в необходимом объеме. Остальному командному составу конкретные задачи ставились лишь за сутки или двое до начала наступления... Переписка, телефонные и телеграфные переговоры о готовившемся наступлении запрещались»[11].

Для осуществления скрытности операции советское военное руководство проводило мероприятия по дезинформации противника. Вся подготовка к наступлению велась под видом усиления оборонительных позиций, немцам навязывали идею о том, что советские войска не собираются наступать. Ставка направила соединениям Сталинградского и соседних фронтов ряд директив о прекращении любых наступательных действий и переходе к жесткой обороне. Эти директивы «были переданы Генеральным штабом по прямому проводу. Они не шифровались, поэтому вскоре стали известны немецкой разведке»[12]. Благодаря этим мероприятиям во время наступления под Сталинградом советскому военно-полити-

ческому руководству удалось добиться стратегической внезапности, что во многом способствовало успеху этой операции.

Во время Сталинградской битвы впервые в ходе Великой Отечественной войны советские войска в массовом порядке вели радиоэлектронную борьбу (РЭБ) – постановку помех на вражеских линиях связи.

Напомним, что сама идея РЭБ родилась на российском флоте в период Русско-японской войны. Первый случай использования методов РЭБ произошел 2 (15) апреля 1904 г. Японцы предприняли очередной обстрел Порт-Артура корабельной артиллерией, вошедший в историческую хронику обороны крепости под названием «третьей перекидной стрельбы». Официальный рапорт контр-адмирала П.П. Ухтомского содержит следующее сообщение:

«В 9 час. 11 мин. утра неприятельские броненосные крейсера “Нисин” и “Касуга”, маневрируя на зюйд-зюйд-вест от маяка Ляотешань, начали перекидную стрельбу по фортам и внутреннему рейду. С самого начала стрельбы два неприятельских крейсера, выбрав позиции против прохода Ляотешаньского мыса, вне выстрелов крепости, начали телеграфировать, почему немедленно же броненосец “Победа” и станции Золотой горы начали перебивать большой искрой неприятельские телеграммы, полагая, что эти крейсера сообщают стреляющим броненосцам о попадании их снарядов. Неприятелем выпущено 208 снарядов большого калибра. Попаданий в суда не было»[13].

Существенное развитие методы РЭБ получили во время Великой Отечественной войны, в частности в период Сталинградской битвы. В декабре 1942 г. Л.П. Берия обратился в Госкомитет обороны СССР с запиской о том, что НКВД считает целесообразным организовать специальную службу по «забиванию» немецких радиостанций, действующих на поле боя. В записке также указывалось: «В частности нам известно, что радиостанции частей германских армий, окруженных в районе Сталинграда, держат связь со своим руководством, находящимся вне окружения, на волнах от 438 до 732 метров»[14]. После одобрения Сталиным предложения Берии в составе внутренних войск НКВД СССР были сформированы радиодивизионы мешающего действия по забивке радиостанций противника на поле боя. В конце 1942 г. Ставка Верховного главнокомандующего приняла решение о создании радиобатальонов специального назначения (РБСН) и в армии. Решением ГКО эта служба была создана в составе отдела радиоразведки Разведывательного управления Генерального штаба, ее возглавил

заместитель начальника отдела М.И. Рогаткин. В конце 1942 – начале 1943 г. были сформированы три, а позднее еще один радиодивизион специального назначения (радиопомех), которые действовали на фронтах до окончания Великой Отечественной войны[15]. Так в огне Сталинградской битвы родилась служба радиопомех, выросшая впоследствии в службу радиоэлектронной борьбы.

Огромную роль в достижении победы под Сталинградом сыграли наши радиоразведчики и криптоаналитики. В первые годы Великой Отечественной войны дешифровальной работой в СССР занимались органы государственной безопасности и ГРУ Генерального штаба Вооруженных сил СССР. Расскажем о деятельности этих организаций в период Сталинградской битвы подробнее. Начнем с военных разведчиков.

Еще в довоенные годы советское руководство приняло решение о создании радиодивизионов особого назначения (ОСНАЗ). Они входили в состав Главного разведывательного управления (ГРУ) Генштаба Красной армии и во время войны вели перехват открытых и шифрованных сообщений немцев и их союзников в прифронтовой полосе, занимались пеленгацией вражеских передатчиков, создавали радиопомехи, участвовали в операциях по дезинформации противника. В каждом батальоне было от 18 до 20 приемников перехвата и 4 пеленгатора[16]. Подготовка персонала для этих подразделений началась в 1937 г. в Ленинграде. Этим занимались на инженерном радиотехническом факультете Военной электротехнической академии связи им. С.М. Буденного.

Летом 1942 г. радиоразведчики научились по изменениям в радиосвязи противника делать оперативные выводы, подчас весьма серьезные. Полковник П.И. Гнутиков, к примеру, вспоминает, как под Харьковом его радиопеленгаторщик безошибочно опознал радиста 17-й танковой дивизии немцев, вышедшего всего один раз в эфир для проверки связи. Обнаружение этой дивизии под Харьковом стало неожиданностью для нашего командования, так как она числилась в резерве совсем на другом направлении.

К исторической Сталинградской битве радиоразведка подошла, обладая бесценным опытом. Непосредственно перед битвой действовали три радиодивизиона. Ими командовали И.А. Лобышев, Н.А. Матвеев, Ф.Н. Слободянюк. В оборонительный период битвы радиоразведка сумела, в частности, вскрыть выход итальянских и румынских частей к Дону, нащупав, таким образом, потенциально слабые места в группировке войск противника. Именно тогда во фронтовых радиодивизионах стали создаваться манев-

ренные группы, которые действовали в передовых подразделениях наших войск, ведя радиоперехват в тактическом звене управления противника. С началом контрнаступления советских войск радиоразведка постоянно освещала положение в гитлеровской армии, перехватывала открытые, подчас панические донесения немцев, что позволяло быстро принимать соответствующие решения. В напряженные декабрьские дни 1942 г. радиочасти ОСНАЗ сумели вовремя разведать сосредоточение в районе Тормосина трех дивизий 48-го танкового корпуса немцев, а в Котельниково – другой ударной группировки в составе трех дивизий 57-го танкового корпуса.

Начав 12 декабря наступление в сторону Сталинграда из района Котельниково, немцы с упорными боями продвигались вперед и, когда расстояние до окруженной группировки Паулюса сократилось до 40 км, начали срочную переброску 17-й танковой дивизии с правого берега Дона в район прорыва с целью развития успеха. Данные об этом маневре были своевременно добыты радиоразведкой и другими видами разведки. К месту будущего сражения устремилась 2-я армия под командованием Р.Я. Малиновского. 23 декабря ожесточенное сражение на реке Мышкова закончилось разгромом немецкой ударной группы.

За образцовое выполнение заданий командования в Сталинградской битве два радиодивизиона ОСНАЗ Донского и Южного фронтов были награждены орденами Красного Знамени. Они стали первыми частями радиоразведки, заслужившими высокие награды.

В 1942 г. в состав Разведуправления Красной армии входила и дешифровальная служба. Сотрудники этого вида разведки в 1942 г. добились значительных результатов. Дешифровальной службой ГРУ было раскрыто 75 шифров немецких вооруженных сил и разведки, в результате чего прочитано свыше 25 000 немецких радиограмм. Полученные таким путем сведения о противнике позволили установить дислокацию свыше 100 штабов соединений, раскрыть нумерацию 200 отдельных батальонов и других частей немецкой армии. В период Сталинградской битвы радиотехническая разведка и дешифровальная служба ГРУ добились значительных успехов. К началу контрнаступления наших войск была вскрыта группировка войск противника перед Юго-Западным, Донским и Сталинградскими фронтами, где вели боевые действия 6-я армия и 4-я танковая армии немцев. В ходе контрнаступления радиоразведка фронтов достаточно полно освещала подготовку

контратак противника, переброску резервов, а также потери в живой силе и технике. В 1942 г. дешифровальная служба Разведуправления Красной армии вскрыла основные немецкие и японские системы общевойсковых, политических и дипломатических шифров, шифры немецкой разведки. Специалистам дешифровальной службы удалось прочитать более 50 тыс. шифртелеграмм противника. В конце ноября, когда кольцо окружения немецко-фашистских войск в районе Сталинграда сомкнулось, радиоразведкой было установлено, что в окружении находились штабы 6-й полевой армии, 4, 8 и 51-го армейских корпусов, 11-го механизированного корпуса, 14-го танкового корпуса, а также шести танковых и механизированных дивизий и 13 пехотных дивизий противника, т. е. группировка окруженных немецких войск была вскрыта полностью.

В ноябре 1942 г., в самый разгар Сталинградской битвы, в соответствии с приказом НКО № 00222 от 23 октября 1942 г. о реорганизации ГРУ ГШ Красной армии дешифровальная служба военной разведки и 8 отдельных радиодивизионов ОСНАЗ были переданы в НКВД, где были созданы полевые управления специальной службы, а дивизионы переформированы в отдельные дивизионы спецслужбы, центральную и отдельную радиостанции войск НКВД. Из Наркомата обороны в органы безопасности были переведены опытные криптографы М.С. Одноробов, Н.В. Пишенин, В.С. Полин, Г.И. Пондопуло, М.И. Соколов, А.Ф. Яценко и другие.

Криптоаналитики органов безопасности активно работали ради победы. Так, к весне 1942 г. было дешифровано 50 тыс. только немецких телеграмм, не считая переписки Румынии и других стран гитлеровской коалиции. В 1942 г. 5-й отдел НКВД СССР, помимо исследования и составления кодов, издания шифрблокнотов для государственных учреждений и др., вел дешифровально-разведывательные работы не только по Германии, но и Афганистану, балканским странам, Бельгии, Великобритании, Ираку, Ирану, Испании, Италии, Китаю, Маньчжоу-Го, странам Скандинавии, США, Турции, Финляндии, Франции, Японии[17].

Победа под Сталинградом стала переломным моментом в ходе войны. При этом среди трофеев оказалось большое количество аппаратуры связи, советские войска захватили 696 радиостанций и 933 телефонных аппарата[18]. В ходе битвы советские войска добыли и ценную криптографическую информацию. Так, 3 января 1943 г. летчик-истребитель 910-го ИАП Виктор Иванов сбил над Сталинградом четырехмоторный Fw-200 «Кондор», в обломках

самолета советские солдаты обнаружили коды, которые использовала окруженная 6-я армия генерала Паулюса[19]. Среди трофеев также оказались три знаменитых шифратора «Энигма», а среди военнопленных оказалось несколько шифровальщиков, которые были привлечены к сотрудничеству.

Кстати, немцы весьма высоко оценивали работу советских дешифровальщиков. В январе 1943 г. специалисты Управления связи вермахта (немецкие сухопутные войска) пришли к выводу о вскрытии «Энигмы» советскими криптоаналитиками, так как в расположении окруженной под Сталинградом группировки немецких войск находилось 26 шифраторов этого типа, а подтвердить факт их уничтожения в условиях окружения не представлялось возможным и имелась вероятность попадания «Энигмы» к русским. Кроме того, среди тысяч пленных, захваченных советскими войсками под Сталинградом, могли оказаться шифровальщики[20]. В дальнейшем немцы применяли усовершенствованный вариант «Энигмы». При этом немецкие связисты отдали должное успехам советских криптоаналитиков, когда в решении, принятом на конференции офицеров связи в 1943 г., записали: «Запрещается каким-либо образом выделять передаваемые по радио послания фюрера»[21].

При рассказе о деятельности советских криптоаналитиков во время Великой Отечественной войны, разумеется, нельзя обойти тему знаменитого немецкого шифратора «Энигма». Еще задолго до начала Второй мировой войны на войсковых линиях связи немцы ввели трехдисковую обратимую машину «Энигма» с постоянным коммутатором. Удельный вес шифрпереписки, зашифрованной этими машинами, составлял в немецкой армии примерно 70%. Исследования машины «Энигма» велись по нескольким направлениям, однако раскрыть ее до конца войны так и не удалось. В ходе боевых действий Второй мировой войны в руки советских специалистов попадали экземпляры основной шифровальной машины Германии, а также ключи к ней.

Трофеи были тщательно изучены. Это дало свои результаты. В конце 1942 г. научные сотрудники специальной группы дешифровальной службы ГРУ с помощью агентуры выявили возможность дешифрования немецких криптограмм, зашифрованных «Энигмой», и приступили к конструированию специальных механизмов, ускоряющих процесс дешифрования. Советские специалисты сумели построить математическую модель немецкого шифратора, выявили слабости, которые могли способствовать процессу дешифрования. Кстати, эта информация была использована при

совершенствовании советских шифрмашин, недостатки, присущие «Энигме», были исключены в принципе. Заслуги отечественных криптоаналитиков отражены в представлении к награждению орденами группы офицеров дешифровальной службы военной разведки, которое было подписано начальником ГРУ генералом И. Ильичевым 29 ноября 1942 г. К наградам были представлены 14 офицеров: полковник Ф.П. Малышев, подполковник А.А. Тюменев и капитан А.Ф. Яценко – к ордену Красного Знамени; майор И.И. Уханов, военинженеры 3 ранга М.С. Одноробов и А.И. Баранов, а также капитан А.И. Шмелев – к ордену Красной Звезды. Были награждены и другие офицеры[22]. Однако дешифровать удалось только старые радиоперехваты, потому что в январе 1943 г. немцы ввели ряд дополнительных уровней защиты. Преодолеть эти новинки в тот период советские криптоаналитики не смогли из-за отсталости электронной техники.

Вообще следует отметить, что от определения того, можно ли вообще дешифровать роторную шифрмашину, до практических результатов – дистанция огромного размера. Из косвенных источников можно сделать вывод, что советским криптоаналитикам удавалось эпизодически вскрывать некоторые сообщения, однако о массовом чтении «Энигмы» в СССР говорить нельзя. Но это было закономерно, так как наши криптографы не обладали той исходной информацией, которая имелась у англичан, а также из-за отсутствия достаточных человеческих и материальных ресурсов и слабого развития машинных средств обработки информации. Д. Кан[23] и другие источники, утверждающие о постоянном практическом дешифровании «Энигмы» советскими специалистами, ошибаются.

А теперь самое главное – огромный массив информации, касающейся дешифрования англичанами «Энигмы», в первую очередь содержание дешифрованных криптограмм, советское руководство получало по линии агентурной разведки. Исходя из этого, разумно предположить, что руководители СССР и отечественных дешифровальных служб приняли решение не тратить наши весьма ограниченные силы на «Энигму», так как в данном случае за нас всю необходимую работу делали англичане. Основное внимание советские криптографы уделяли армейским «ручным» шифрам и кодам Германии, а также шифрмашинам других типов, и на этом поприще им удалось достичь значительных результатов[24]. Отметим, что премьер-министр Великобритании У. Черчилль распорядился передавать в СССР разведывательные материалы, полученные из дешифрованных немецких сообщений (большей частью за-

шифрованных «Энигмой»). Сообщения шли со ссылкой на агентурные источники, представителей нейтральных стран, показания пленных и т. д. Любые детали, которые могли бы свидетельствовать о том, что информация получена в результате дешифрования, исключались. Такое сотрудничество продолжалось до конца 1942 г., после чего англичане его почти прекратили. Исключения были сделаны во время Сталинградской и Курской битв, когда информация вновь поступала, но с 1944 г. дешифрованные материалы официальным путем полностью прекратили поступать в СССР. Однако благодаря работе советских агентов вся информация, касающаяся СССР, получаемая англичанами в результате дешифрования «Энигмы», была доступна советскому руководству[25].

В заключение отметим, что подвиги советских специалистов-криптографов, рядовых войсковых шифровальщиков, связистов, радиоразведчиков, специалистов по дешифрованию не забыты и благодарная память о тех, чья жизнь и служба в силу специфики профессии прошла под грифом «особой важности», живет. Ценная информация, добытая героями невидимого криптографического фронта, позволила сохранить жизни тысяч и тысяч наших солдат и офицеров, сыграла значительную роль в победе над врагом.

Примечания

[1] См.: Наука и технологии России – STRF.ru [Электронный ресурс] [М., 2009]. URL: http://www.strf.ru (дата обращения: 07.05.2009).

[2] *Астрахан В.И., Павлов В.В., Чернега В.Г., Чернявский Б.Г.* Правительственная электросвязь в истории России. Ч. I (1917–1945). М.: Наука, 2001. С. 60–61.

[3] Там же. С. 83–84.

[4] Там же. С. 88–90, а также: Наука и технологии России // STRF. ru.

[5] Владимир Александрович Котельников (1908–2005) знаменитый русский ученый, академик АН СССР, дважды Герой Социалистического Труда, лауреат многочисленных премий. В.А. Котельников опубликовал фундаментальные труды в области радиотехники, теории помехоустойчивой связи, радиолокации, радиоастрономии. Впервые в мире сформулировал и доказал фундаментальную теорему дискретизации, на которой основана вся цифровая обработка сигналов. Под его руководством в 1930-е годы были созданы первые отечественные аппараты для шифрования речевого сигнала. Эта работа продолжалась и в годы Великой Отечественной войны. Параллельно с К. Шенноном В.А. Котельников математически формализовал требования к стойкости шифров.

[6] См.: *Быховский М.А.* Круги памяти (Очерки истории развития радиосвязи и вещания в XX столетии). М.: Междунар. центр науч. и техн. инф.; Мобильные коммуникации, 2001. 224 с. См.: *Быховский М.А.* и др. В.А. Котельников и его влияние на научные исследования и разработки ученых НИИР // Электросвязь. №11. 2003; *Быховский М.* Пионеры информационного века. История развития теории связи. М.: Техносфера, 2006.

[7] См.: *Синявская С.* Три дивизии за шифр [Электронный ресурс] // Электронное издание «Наука и технологии России» – STRF.ru [М., 2009]. URL: http://www.strf.ru (дата обращения: 08.05.2009). Подробнее о работе советской шифровальной службы во время Великой Отечественной войны можно прочитать в ряде статей: *Бабиевский В.В., Бутырский Л.С., Ларин Д.А., Шанкин Г.П.* Криптографический фронт Великой Отечественной. Советская шифровальная служба // Защита информации. INSIDE. 2010. № 5. С. 87–96; № 6. С. 74–86; *Ларин Д.А.* О вкладе советских криптографов в Великую победу // Проблемы отечественной истории: Сб. науч. ст. Вып. 13. М.: РАГС, 2010. С.76–85; *Ларин Д.А.* Советская шифровальная служба в годы Великой Отечественной войны // Известия Уральского гос. ун-та. Сер. 1. Проблемы науки и образования. 2011. № 1 (86). С. 69–80.

[8] *Барятинский М.* Битва за Сталинград. М.: Яуза; Коллекция; Эксмо, 2007. С. 22.

[9] Там же.

[10] Там же.

[11] Там же. С. 36.

[12] Там же. С. 21.

[13] Телекоммуникационное право. История. Из истории радиоэлектронной борьбы. [Электронный ресурс] [М., 2011]. URL: http://www.telecomlaw.ru (дата обращения: 08.09.2011).

[14] См.: *Лобанов Б.С.* 65-летию Победы посвящается. [Электронный ресурс] // Сайт Российской академии естественных наук. [М., 2010] URL: http://www.raen.info/press/faces/document3058.shtml (дата обращения: 08.09.2010).

[15] См.: Там же.

См.: *Ржевцев Ю.П.* Радиодивизионы ОСНАЗ и отдельные дивизионы специальной службы внутренних войск НКВД СССР [Электронный ресурс] // Сайт «Книга памяти Калининградской области» [Калининград, 2008] URL: http://may1945-pobeda.narod.ru/nkvd-ruf.htm, (дата обращения: 08.09. 2008).

[16] *Анин Б.А., Петрович А.И.* Радиошпионаж. М.: Международные отношения, 1996. С. 282.

[17] См.: *Ильичев А.* Мой дед был начальником ГРУ. [Электронный ресурс] // Сайт «Наша Победа» [М., 2005] URL: http://www.9may.ru/ (дата обращения: 08.09.2011).

См.: *Корабельников В.* Роль и место военной разведки в достижении победы в Великой Отечественной войне 1941–1945 годов. [Электронный ресурс] [М.,

2007] URL: http://vybory.org/articles/479.html (дата обращения: 08.09.2011); *Кузьмин Л.А.* Не забывать своих героев // Защита информации. Конфидент. 1998. № 1. С. 83–85; *Кузьмин Л.А.* ГУСС (этап в развитии советской криптографии // Защита информации. Конфидент. 1998. № 4. С. 89–94; *Кузьмин Л.А.* Становление кафедры криптографии // Защита информации. Конфидент. 1999. № 1–2. С. 85–90; Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945: Сб. док. [Электронный ресурс] [М., 1995] URL: http://mosohin.ru (дата обращения: 18.01.2011); *Серов Е., Волгин В.* Тайны военной разведки (1918–1945) // Армия. 1993. № 20. С. 53–56; № 21. С. 49–55; 1994. № 7. С. 52–55; Официальный сайт РООВСОЗИ «Сфинкс-79» (Региональная общественная организация ветеранов специальных органов защиты информации, являющаяся коллективным членом Общероссийской организации ветеранов войны и военной службы). [Электронный ресурс] [М., 1995] URL: http://www.sfinxclub.ru (дата обращения: 18.01.2011).

[18] *Барятинский М.* Указ. соч. С. 92.

[19] См.: Советские асы на истребителях лендлиза / Ред.-сост. С.В. Иванов. Белорецк: Нота, 2005.

[20] *Анин Б.А., Петрович А.И.* Указ. соч. С. 281; *Межутков А.* Исторический экскурс // Практическое руководство по методам и средствам криптографической защиты информации. М.: DigitalSecurity 2003; Разведдаты января // Независимое военное обозрение. 2002. № 45. С. 7.

[21] *Кан Д.* Война кодов и шифров. М.: РИПОЛ КЛАССИК, 2004. С. 236.

[22] *Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П.* Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 5. Накануне // Защита информации. INSIDE. 2006. № 5. С. 76; Ч. 6. Первый экзамен выдержан! // Там же. № 6. С. 86; *Ильичев А.* Указ. соч.; *Корабельников В.* Указ. соч.; *Кузьмин Л.А.* Указ. соч.; *Лота В.* Секретный фронт Генерального штаба // Красная звезда. 2002. 2 нояб.; Органы государственной безопасности СССР в Великой Отечественной войне 1941–1945: Сб. док. [Электронный ресурс] [М., 1995] URL: http://mosohin.ru (дата обращения: 18.01.2011); *Серов Е., Волгин В.* Указ. соч.; Официальный сайт РООВСОЗИ «Сфинкс-79» [Электронный ресурс] [М., 1995] URL: http://www.sfinxclub.ru (дата обращения: 18.01.2011).

[23] См.: *Кан Д.* Указ. соч.

[24] См.: Г*ольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П.* Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
См.: *Лайнер Л.* Погоня за «Энигмой». М.: Молодая гвардия, 2004.
См.: *Ларин Д.А., Шанкин Г.П.* Вторая мировая война в эфире: Некоторые аспекты операции «Ультра» // Защита информации. INSIDE. 2007. № 1. С. 91–96; 2007. № 2. С. 87–96.

[25] Там же.

С.В. Запечников

ИЗ ИСТОРИИ КРИПТОГРАФИИ: ВКЛАД ЛЕОНАРДА ЭЙЛЕРА В СТАНОВЛЕНИЕ МАТЕМАТИЧЕСКИХ ОСНОВ СОВРЕМЕННОЙ КРИПТОЛОГИИ

Эта статья – одна из серии исторических очерков и одновременно попытка науковедческого анализа одного из самых блестящих периодов отечественной и мировой науки, связанного с жизнью и деятельностью великого математика, механика и физика Леонарда Эйлера. В статье раскрываются научные и творческие методы Л. Эйлера и его роль в становлении теории чисел, анализируются пути использования его результатов современной наукой, рассматриваются некоторые аспекты истории создания отечественной системы математического образования. Особое внимание уделяется значимости трудов Л. Эйлера для современной асимметричной криптографии (криптографии с открытым ключом) и теории криптографических протоколов.

Ключевые слова: история криптографии, теория чисел, простые числа, вычислительно сложные задачи, математическое образование.

Одна из самых ярких страниц истории российской и мировой науки связана с именем Леонарда Эйлера. Универсальный ученый, работавший в самых разных отраслях знания: фундаментальной и прикладной математике, механике, гидродинамике, оптике и многих других – особенно большой вклад внес в развитие теории чисел. Теория чисел стала фундаментом современной криптологии (криптографии и криптоанализа): многие методы теории чисел ныне являются классическими инструментами конструирования и анализа криптографических механизмов защиты информации. В наше время средства криптографической защиты стали традиционными, привычными составляющими

систем защиты информации. Вместе с тем нередко специалисты в этой области, а тем более пользователи компьютерных систем, имеют слабое представление о том, какой долгий и трудный путь прошли криптология и криптоанализ, прежде чем оформились в виде современных составляющих науки об информационной безопасности, какие фундаментальные открытия в области математики послужили стимулом к разработке на их основе методов защиты информации.

Леонард Эйлер – один из таких людей, без которых не было бы криптологии в ее современном виде. Первое, на что обращает внимание исследователь, пытаясь оценить вклад Л. Эйлера в науку, – исключительно высокое качество его научных результатов. Разумеется, продукт труда любого ученого – это открытые им объективные закономерности реального мира, но форма представления этого продукта, степень его универсальности, даже принятые термины и обозначения, конечно, зависят от того, «из чьих рук они вышли». И в этом смысле плоды научного труда Л. Эйлера отличаются поразительной красотой, цельностью и лаконичностью при одновременной отделанности каждой детали. Конечно, не будь Эйлера, открытые (сформулированные) им объективные законы рано или поздно были бы открыты кем-то другим, но, возможно, они не были бы столь красивыми и совершенными, какими мы их знаем, и математика в целом, а прикладная математика и криптология в частности, не обладали бы значительной долей присущей им красоты.

Эти размышления вызвали у автора сначала желание, а потом все острее сознаваемую необходимость обратиться к изучению научного наследия великого математика, механика и физика Л. Эйлера в рамках цикла исследований по истории криптографии[1].

Настоящая статья является второй из серии задуманных автором работ, посвященных наиболее значимым и интересным, а подчас и малоизученным страницам истории отечественной и зарубежной криптографии.

Автор надеется, что материалы его работ по истории криптографии будут содействовать пробуждению интереса учащихся и преподавателей к изучению криптографии не только в теоретическом, но и в историческом аспекте. Это плодотворно для любой науки, но из примеров, которые нам дает история криптографии, есть возможность извлечь особенно много полезного, учитывая ее богатейшее прошлое и «всепроникающий» характер (хотя чаще всего и скрытый от посторонних глаз).

1. Краткий очерк жизни и деятельности Л. Эйлера

Леонард Эйлер – явление в мировой науке исключительное. Его по праву называют самым великим математиком XVIII в. И мы должны гордиться тем, что этот великий ученый в свое время выбрал Россию, а именно Петербург, императорскую Академию наук как основное место своей профессиональной деятельности. Здесь он проработал почти половину жизни: в общей сложности 31 год из отпущенных ему судьбой 76 лет.

Леонард Эйлер родился в швейцарском городе Базеле 4 апреля 1707 г. в семье пастора Пауля Эйлера. Обучение начинал под руководством отца, который готовил его к духовной карьере, одновременно занимаясь с ним математикой для развития логического мышления. Сам Пауль Эйлер некогда учился математике у знаменитого Якоба Бернулли – одного из основателей теории вероятностей и математического анализа, профессора Базельского университета, учителем которого был Лейбниц. Уже в 13 лет Л. Эйлер также становится студентом Базельского университета. Его научным руководителем был Иоганн Бернулли младший брат Якоба Бернулли. В 1724 г. Л. Эйлер получает ученую степень магистра, а в следующем году пишет диссертацию на замещение вакантной должности профессора физики в этом университете (в то время так было принято), однако в число кандидатов его не включили из-за слишком юного возраста. Число научных вакансий в европейских университетах было невелико, поэтому сыновья Иоганна Бернулли – Даниил и Николай, воспользовавшись выгодным предложением недавно организованной в России императорской Академии наук, уехали в Санкт-Петербург. По их совету и с их помощью после решения многочисленных организационных и финансовых вопросов в 1727 г. Л. Эйлер также прибывает в Санкт-Петербург и приступает к работе в должности адъюнкта кафедры физиологии. По словам М. Кондорсе[2], «они употребили столько же усилий для того, чтобы приблизить к себе своего страшного соперника, сколько их употребляют обыкновенные люди для удаления такового».

В 1731 г. Л. Эйлер получает освободившееся место профессора физики в Петербургской академии. Он много и напряженно работает, занимаясь как важными правительственными заданиями, так и рядом инициативных исследований, выступает с лекциями, делает доклады на академических конференциях. До 1741 г. он уже опубликовал более 90 крупных научных работ. После 1736 г.

Эйлер становится широко известен в Европе благодаря своей выдающейся монографии «Механика, или наука о движении в аналитическом изложении».

В 1741 г., после существенного ухудшения положения дел в Российской академии наук, Эйлер подает прошение об отставке, принимает приглашение короля Пруссии Фридриха II и переезжает в Берлин. В Пруссии он также активно занимается наукой и практической деятельностью. С 1748 по 1766 г. выходят в свет его важнейшие монографии: «Введение в анализ бесконечно малых», «Морская наука», «Теория движения Луны», «Наставление по дифференциальному исчислению», «Теория движения твердых тел», «Элементы вариационного исчисления». Начиная с 1759 г. король поручает ему руководство Прусской академией наук, правда, без титула президента.

В 1762 г. на русский престол вступает Екатерина II, проводившая, как известно, политику просвещенного абсолютизма. Она сразу же посылает Эйлеру приглашение вернуться в Российскую академию наук на любых условиях. После многократных ходатайств Екатерины II король Фридрих II в 1766 г. наконец отпускает Эйлера в Петербург. В июле того же года он прибывает в Россию навсегда. По приезде он приобретает дом в Петербурге на Васильевском острове, где проживает до конца жизни (дом сохранился, нынешний его адрес: наб. Лейтенанта Шмидта, 15). За второй период пребывания в России он подготовил более 400 статей и 10 книг. Важнейшие его работы этого периода: «Универсальная арифметика» (2 тома), «Оптика» (3 тома), «Интегральное исчисление» (3 тома), «Новая теория движения Луны», «Всеобщая сферическая тригонометрия». Эйлер активно трудился и сохранял феноменальную память до последних дней. Авторитет его среди российских и европейских ученых был непререкаемым.

Скончался Л. Эйлер 7 сентября 1783 г. от кровоизлияния в мозг. «Он перестал вычислять и жить», – сказал М. Кондорсе на траурном заседании Парижской академии наук. Эйлер был похоронен на Смоленском лютеранском кладбище. В 1955 г. его прах был перенесен в «Некрополь XVIII в.» на кладбище Александро-Невской лавры.

Эйлер завещал публиковать его труды в изданиях Петербургской академии наук в течение 20 лет после его смерти. На деле количество оставленных им и не опубликованных при жизни работ было столь велико, что они печатались в течение 42 лет после его кончины. Жизнь и деятельность Эйлера – замечательный пример

интернациональности науки как в его время, так и в наши дни, когда учеными разных стран тщательно, по крупицам собирается, систематизируется и обрабатывается его драгоценное научное наследие.

Наследие Эйлера для мировой науки поистине бесценно, ведь по существу он явился основоположником целого ряда математических наук: аналитической теории чисел, вариационного исчисления, теории функций комплексного переменного, дифференциальной геометрии поверхностей, аналитической механики, динамики твердого тела, а также многих разделов теории дифференциальных уравнений, теории алгоритмов, теории эллиптических функций, небесной механики и других отраслей «чистой» и прикладной математики. Ученый обладал энциклопедическими знаниями: его интересы распространялись еще и на многие области астрономии, акустики, оптики, статистики, ботаники, медицины, химии, лингвистики, музыки, инженерного дела.

Только в области «чистой» математики с именем Эйлера связаны: задача Эйлера («задача о кенигсбергских мостах»), метод ломаных Эйлера, подстановка Эйлера, постоянная Эйлера, произведение Эйлера, прямая Эйлера, знаменитая теорема Эйлера о многогранниках, три вида дифференциальных уравнений Эйлера, по крайней мере шесть формул Эйлера, относящихся к разным областям математики (знаменитая тригонометрическая формула $e^{ix} = \cos x + i \sin x$, разложение функции $\sin x$ в бесконечный ряд, тождество о пятиугольных числах, тождество о простых числах, тождество о четырех квадратах, формула о кривизнах), арифметическая функция Эйлера $\varphi(n)$, круги Эйлера (метод решения теоретико-множественных и логических задач), призма Эйлера, числа Эйлера, бета-функция и гамма-функция Эйлера, а также «неберущиеся» Эйлеровы интегралы, Эйлеровы углы, Эйлеров сферический треугольник, Эйлерова характеристика. Наконец, в честь ученого, установившего понятие о логарифмировании как действии, обратном возведению в степень, обозначается буквой e + 2,71828... одна из важнейших математических констант – основание натурального логарифма.

Пожалуй, важнейшая черта трудов Эйлера и одновременно важнейшее их значение для науки состоят в том, что вся его деятельность была направлена не просто на установление единичных научных фактов, не просто на решение тех задач, которые у него «хорошо получались», а на построение системы нового научного знания с ядром в виде системы математических инструментов.

Эйлер как никто другой чувствовал и раскрывал в своих научных трудах красоту математики.

2. Творческие и научные методы Л. Эйлера

Представляют несомненный интерес те творческие и научные методы Л. Эйлера, которые позволяли ему добиваться таких выдающихся результатов в столь разных областях научного знания.

Прежде всего обращает на себя внимание поразительная работоспособность великого ученого. За 56 лет его научной деятельности (от первых работ 1726–1727 гг. и вплоть до смерти в 1783 г.) число его научных трудов превысило 860 наименований. Несложный подсчет показывает, что в среднем он создавал по одной научной работе каждые 3–4 недели. А ведь среди них были не только статьи, насыщенные математическими выкладками, но и монографии, и учебники огромного объема, в том числе многотомные. Такая производительность научного труда при таком его качестве почти немыслима даже для современных ученых, обладающих целым арсеналом средств автоматизации научных исследований и офисной работы. К этому следует добавить еще и то обстоятельство, что, выполняя свой долг ученого, он совершил и великий человеческий подвиг: несмотря на то что в возрасте 31 года он потерял зрение на один глаз из-за кровоизлияния, а в возрасте 59 лет его постигла полная слепота, работоспособность Эйлера на протяжении всей жизни практически не снижалась. Таким образом, первый принцип Эйлера заключался в постоянном и неустанном труде, вне зависимости от таких важнейших для каждого человека факторов, как состояние здоровья, материальное благополучие и окружающая политическая обстановка.

Кроме того, выше уже отмечалась редкая разносторонность его научных дарований. Действительно, с трудом можно найти такую отрасль естествознания или прикладной науки, которую он оставил бы без внимания. Выражаясь современным языком, в его «портфолио» входили труды по дифференциальному и интегральному исчислению, теории чисел, вариационному исчислению, теоретической механике, гидродинамике, оптике, баллистике, теории упругости, теории машин, морской науке, судостроению и кораблевождению, страховому делу, теории музыки и многим другим наукам. В связи с этим возникают закономерные вопросы: Как ученый мог «переключаться» с одной задачи на другую? Занимался ли он разными задачами параллельно или последовательно?

В какой мере решаемые им научные проблемы оказывали влияние друг на друга?

Ключ к разрешению этих вопросов следует искать путем анализа содержания и последовательности созданных Эйлером на протяжении достаточно длительного интервала времени научных трудов. Один из привлекательных примеров для такого анализа – сборник “Lettres à une princesse d’Allemagne sur divers sujets de physique et de philosophie”. Знакомство с этим уникальным письменным памятником (в русском переводе)[3] позволяет проследить день за днем ход научного поиска Л. Эйлера на протяжении более чем двух лет. Всего в сборник входит 234 письма, самое раннее из которых датируется 19 апреля 1760 г., самое позднее – концом мая 1762 г. Тематика писем «плавно» меняется, переходя от одной отрасли науки к другой через близкие или связанные друг с другом проблемы. Вот пример: письма с 3 по 8, написанные в период с 26 апреля по 6 мая 1760 г. (то есть в течение 11 дней), посвящены музыке («О звуке и его скорости», «О консонансах и диссонансах», «Об унисоне и октаве», «О других созвучиях», «О двенадцати тонах клавесина», «Об удовольствии, доставляемом хорошей музыкой»), Следующее же, 9-е письмо он начинает словами: «Объяснение природы звука... приводит меня к необходимости рассматривать более подробно свойства воздуха, способного испытывать такие же колебательные движения, как и звучащие тела: струны, колокола и т. п., и передавать эти колебания нашим ушам. Возникает вопрос, что же представляет собой воздух?»[4] И следующие письма (с 9-го по 16-е) посвящены преимущественно аэростатике и проблемам атмосферных явлений. Период «увлечения» этой тематикой длится у Эйлера 24 дня, с 10 мая по 3 июня 1760 г. Изучение физики атмосферы логично подводит Эйлера к следующему вопросу, сформулированному в 17-м письме: «После того как я уже столько говорил о солнечных лучах (в атмосфере. – *С. З.*), этом источнике тепла и света ... без сомнения, возникает вопрос: что представляют собой солнечные лучи? Бесспорно, это одна из наиболее важных проблем физики...»[5] Дальнейшие письма (с 17 по 44) представляют собой достаточно глубокое проникновение в задачи оптики. Этот период длился с 7 июня по 21 августа 1760 г., т. е. в течение 76 дней. В последующих письмах Л. Эйлер обращается к проблемам гравитации (письма 45–50, написанные с 23 по 30 августа того же года, период – 9 дней), после чего «незаметно» переходит к проблемам небесной механики (письма 51–68, с 1 сентября по 18 октября, период – 48 дней),

а от них – к физическим основам кинематики и динамики, включая определение понятий движения, силы, веса, инерции и других основополагающих для физики понятий (письма 69–79, с 21 октября по 25 ноября, период – 36 дней). Вторая часть «Писем к немецкой принцессе...» посвящена (последовательно) проблемам религиозной философии, лингвистики, логики, этики, учению об атомах и молекулах, и, наконец, электричеству. Столь же разносторонни и письма из третьей части сборника.

Таким образом, на примере анализируемого собрания сочинений Эйлера можно сделать вывод о важнейшем научном и творческом принципе Эйлера – непрерывном и поступательном движении его мысли «по спирали» от одной проблемы к другой с неоднократным возвращением к уже «пройденным» отраслям знания, но на новом качественном уровне с учетом вновь выявленных фактов и обнаруженных закономерностей. Это движение мысли основывалось на ясном видении многогранности и взаимосвязанности всех явлений как окружающего мира, так и внутреннего мира человека. Важнейшим «двигателем» Эйлера по пути научных изысканий была неослабевающая потребность в самообразовании, в чем он видел одну из высших ценностей человеческой жизни.

Характернейшей чертой научных сочинений Эйлера, которая также прекрасно прослеживается в «Письмах к немецкой принцессе...» и которую мы отметим в качестве третьего творческого принципа, является предельная ясность, доступность, логичность и выверенность изложения мыслей. Именно благодаря этому «Письма к немецкой принцессе...» в XVIII–XIX вв. выдержали более 100 изданий на разных языках и служили своего рода энциклопедией естественно-научных и гуманитарных знаний. То же качество характерно практически для всех сочинений Эйлера. В отличие от многих других ученых и естествоиспытателей его (да и нашего) времени, он в своих работах отнюдь не ограничивался изложением готового результата исследований, состоявшегося научного факта. Он старался так изложить ход своих мыслей, чтобы читатель вслед за автором и вместе с ним прошел весь путь научного открытия: от зародившегося вопроса «почему» через анализ и сопоставление фактов, обоснование путей решения проблемы, ряд умозаключений к ответу на вопрос и постановке нового вопроса, опираясь на только что полученный результат. Этим ученый стремился передать свой дух постоянного творческого «горения» читателю и увлечь его самостоятельным исследо-

ванием новых и новых задач. Вот почему значение работ Эйлера не ограничивается только содержащимися в них научными результатами: они служат своего рода образцовой творческой, учебно-исследовательской лабораторией ученого, в какой бы области знания он ни работал.

Четвертым в перечне научных и творческих принципов Л. Эйлера следовало бы назвать тесную связь, даже «сплав» в его сознании научного и религиозного мировоззрения. Эйлер рассматривал занятия наукой не иначе как приближение человека к Богу, движение по пути постижения замысла Творца, а полученный продукт – научное знание – как добытую человеком частицу бесконечной мудрости Божией. Не останавливаясь подробно на комментировании этого тезиса, процитируем одну, быть может, малоизвестную, но показательную историю[6]: «Тьебо (Thiebault) рассказывает, что к Российскому двору был приглашен Дидро, который, будучи атеистом, стал распространять свои идеи. Чтобы заставить его замолчать, был придуман план. Эйлер, истинно верующий христианин, подошел к Дидро и провозгласил по-французски: "$(a + b^n)/n = x$, следовательно, Бог существует! Отвечай!" Дидро не знал математики, поэтому молчал. Поднялся хохот, отчего Дидро смутился настолько, что немедленно вернулся во Францию». Живой ум в сочетании с непоколебимой уверенностью в силе физико-математического знания позволяли Эйлеру уверенно браться за решение любых самых сложных научных проблем.

Наконец, важнейшей чертой творческого метода Эйлера была его обращенность не только к прикладным задачам и практическим потребностям. Ни одна из решаемых им научных задач не была оторванной от жизни «наукой ради науки» – напротив, большинство из них было вызвано потребностями общественной жизни. Однако в своих исследованиях Эйлер почти всегда проникал в суть проблемы столь глубоко, что получал фундаментальные научные результаты. Так было и с теорией чисел.

3. Основные результаты исследований Л. Эйлера в области теории чисел

Практически все результаты Л. Эйлера, принадлежащие тем областям математики, которые формируют математические основы современной криптологии, концентрируются вокруг теории чисел. Назовем только самые значительные его заслуги в этой области. Эйлер является основоположником аналитической теории

чисел, он доказал и обобщил малую теорему Ферма, впервые высказал гипотезу о справедливости квадратичного закона взаимности, ввел в рассмотрение ряд арифметических функций, включая знаменитую дзета-функцию (правда, сегодня она известна как дзета-функция Римана), ввел понятие первообразного корня, доказал многочисленные теоремы, леммы, утверждения, вывел формулы, ныне носящие его имя. Всего теории чисел посвящено более 120 работ Эйлера. П.Л. Чебышев писал: «Эйлером было положено начало всех изысканий, составляющих общую теорию чисел». Теоретико-числовые работы Эйлера подробно рассмотрены историками математики[7], поэтому далее мы остановимся только на тех работах, которые впоследствии пригодились в криптографии.

Эйлер «заразился» теоретико-числовыми исследованиями от Христиана Гольдбаха, служившего, кстати сказать, криптографом в Министерстве иностранных дел в Москве[8] (криптограф-иностранец на службе в дипломатическом ведомстве – ситуация, немыслимая в наше время!). Эйлер начал свою работу в области теории чисел с доказательства ложности утверждения Ферма о том, что все числа вида $2^{2^m} + 1$, $m = 1, 2, ...$ (так называемые числа Ферма) – простые: он нашел делитель такого числа при $m = 5$. Однако это была единственная найденная им ошибка Ферма, в дальнейшем Эйлер доказал почти все остальные теоретико-числовые предположения Ферма. Впоследствии Эйлер снова возвращался к числам Ферма, работая над проблемой отыскания простых чисел. Он доказал теорему, что не существует такой целой функции, все значения которой при целых значениях аргумента были бы простыми числами. Эйлер исследует на простоту числа вида $2^{2^n} - 1$, $n = 1, 2, ...$ (так называемые числа Мерсенна), находит делители некоторых из них, интуитивно нащупывает (но не доказывает) теорему о том, что разность $a^n - b^n$ всегда делится на $n + 1$, если $n + 1$ – простое число, и $n + 1$ не является делителем a либо b. От этого исследования он переходит к доказательству малой теоремы Ферма[9]: $a^{p-1} \equiv (\mathrm{mod}\ p)$. Эйлер дает четыре различных доказательства теоремы Ферма в работах 1741, 1750, 1761, 1764 гг., при этом доказывает более общую теорему, ставшую знаменитой как *теорема Эйлера*:

$$a^{\varphi(n)} \equiv (\mathrm{mod}\ p) \qquad (1)$$

где $\varphi(n)$ – впервые употребленная Эйлером числовая функция, впоследствии также названная его именем, которая выражает количество чисел, взаимно простых с n и не превосходящих n. Теорема Ферма вытекает из этой теоремы как частный случай.

Эта теорема стала первой вершиной теоретико-числовых исследований Эйлера.

С доказательства малой теоремы Ферма Эйлер начинает заниматься теорией квадратичных вычетов[10]. Он рассматривает остатки, получающиеся при делении квадратов на простое число p, – *квадратичные вычеты* ($a \in Q_p$). Он замечает, что помимо этих чисел существуют и другие числа, меньшие p и не попадающиеся среди остатков, – это *квадратичные невычеты* ($a \in \overline{Q}_p$). Исследования в этой области приводят его в 1750 г. к формулированию важнейшего утверждения, известного теперь как критерий Эйлера:

$$\left(\frac{a}{b}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p), \qquad (2)$$

где p – нечетное простое число, a – целое число, $\left(\frac{a}{b}\right)$ – символ Лежандра, определяемый таким образом:

$$\left(\frac{a}{b}\right) = \begin{cases} 0, \text{ если } p \mid a, \\ 1, \text{ если } a \in Q_p \\ -1, \text{ если } a \in \overline{Q}_p. \end{cases}$$

В частности, $\left(\frac{1}{p}\right) = 1$ и $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Следовательно, $-1 \in Q_p$, если $p \equiv 1(\mathrm{mod}4)$, и $-1 \in \overline{Q}_p$, если $p \equiv 3(\mathrm{mod}4)$. И это был еще один важнейший для теории чисел результат.

Эйлер исследует в 1742–1749 гг. числа специального вида: дружественные, многоугольные, удобные, обобщенные простые и другие, а также свойства некоторых важных арифметических функций, в частности функции $\sigma(n)$ – суммы делителей числа n. В этот же период он дает эскиз доказательства теоремы о многоугольных числах, рассматривает теорему о двух квадратах и связанные с ней утверждения и теоремы, а затем теорему о четырех квадратах. Таким путем в 1751 г. он приходит к следующей вершине своих изысканий – *квадратичному закону взаимности*: если q – нечетное простое число, отличное от p, то

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot \left(-1\right)^{\frac{(p-1)(q-1)}{4}} \qquad (3)$$

Одновременно после доказательства малой теоремы Ферма начинаются исследования Эйлера по теории степенных вычетов. В одной из работ 1774 г. он вводит понятие первообразного корня

(radix primitiva), доказывает существование первообразного корня для любого простого числа и определяет количество первообразных корней. Напомним, что *показателем*, которому принадлежит число a по mod$m$, называется минимальное γ: $a^{\gamma} \equiv 1 (\mathrm{mod} m)$. Говорят и по-другому: показатель числа a по mod$m$. В частном случае, когда порядок числа a равен $\varphi(m)$, a называется *первообразным корнем* по mod$m$. По одному и тому же модулю бывают разные первообразные корни. Как состоялось это открытие[11]? Рассматривая остатки от деления членов геометрической прогрессии 1, a, a^2, a^3, a^4, ... на взаимно простое с a число p, он замечает, что иногда эти остатки совпадают со всеми натуральными числами, меньшими p, а иногда – только с некоторыми из них, и выясняет, что число различных остатков является делителем числа $p-1$. Число, порождающее полный ряд вычетов, Эйлер и назвал первообразным корнем делителя p, а далее доказал, что если a – первообразный корень, то a^{p-1} при делении на простое число p дает остаток, равный 1. Главная его *теорема о существовании первообразного корня* звучала так: «Какое бы простое число ни было взято в качестве делителя p, всегда можно найти такую геометрическую прогрессию 1, a, a^2, a^3, a^4, ... и т. д., из которой будет возникать полный ряд вычетов». Эйлер впервые рассчитывает таблицу первообразных корней для всех $p \leq 37$. И это была еще одна теоретико-числовая вершина Эйлера.

Продолжая образные сравнения, можно сказать, что эти результаты сами по себе были вершинами, но они были вершинами высокой горной цепи, так как и другие открытия Эйлера представляют не меньшую ценность (но уже для других разделов прикладной математики, поэтому мы перечислим их совсем кратко). В разные годы Эйлер ведет поиски способов распознавания (отыскания) простых чисел, больших любого заданного, составляет таблицы простых чисел. Еще одно важное направление его исследований – диофантов анализ – решение неопределенных уравнений в целых числах. Наконец, как уже говорилось, важнейшей заслугой Эйлера было создание аналитической теории чисел. Как пример блестящего применения методов математического анализа для доказательства теоретико-числовых утверждений можно указать замечательное тождество Эйлера для дзета-функции[12]. Дзета-функция определяется рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (4)$$

Из курса математического анализа известно, что ряд (4) сходится при всех действительных $s > 1$ и расходится при $s \le 1$. Такие ряды при различных целых значениях s изучал Л. Эйлер. Впоследствии дзета-функция стала рассматриваться обобщенно как функция действительного переменного $s > 1$. Ее свойства тесно связаны со свойствами множества простых чисел, что позволило Эйлеру использовать для исследования простых чисел методы математического анализа и с их помощью доказать следующую теорему: при каждом $s > 1$ справедливо тождество

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

где p – все последовательно идущие простые числа, $p \ge 2$.

4. Применение научных результатов Л. Эйлера в современной криптологии

В предыдущем разделе речь шла о важнейших теоретико-числовых результатах исследований Эйлера из области «чистой» математики. Рассмотрим теперь их с точки зрения приложения в криптографии. Разумеется, сам Леонард Эйлер не мог предвидеть развития тех методов и направлений криптологии, которые стали привычными для нас и изучаются сейчас в университетских курсах как основа этой науки. Тем не менее в целях удобства основные направления использования результатов Эйлера могут быть сгруппированы по четырем категориям.

1. *Тестирование чисел на простоту*. Самый элементарный тест на простоту – тест Ферма[13] – основан на малой теореме Ферма. Тест основан на понятии *псевдопростого числа по основанию a*: если a и p – взаимно простые числа, такие, что $a^{p-1} - 1$ делится на p, то число p может быть, а может и не быть простым. В случае, когда p составное, оно называется псевдопростым по основанию a. Первое псевдопростое число по основанию 2 нашел Ф. Саррус в 1820 г. – это было число 341. Если тест Ферма определяет число как составное, то оно точно является составным, но если определяет как простое, то оно может быть не простым, а псевдопростым. В этом смысле тест Ферма не дает надежных гарантий простоты чисел, а потому не очень пригоден для использования в криптографии.

Гораздо лучше вероятностный тест Соловея–Штрассена[14] (Solovay–Strassen) – первый тест, который стал использоваться в асимметричной криптографии. Он основан на трех математических

фактах: 1) на критерии Эйлера $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mathrm{mod} n$, где n – нечетное, a – целое, $НОД(a, n) = 1$; 2) на понятии *свидетеля простоты*, или *EW-числа* (Euler witness) для числа n – такого числа a, удовлетворяющего критерию Эйлера, что либо $НОД(a, n) > 1$, либо $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \mathrm{mod} n$; 3) *на понятии псевдопростого числа Эйлера* по основанию n – такого числа a, что $НОД(a, n) = 1$ и одновременно $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mathrm{mod} n$ (т. е. n выглядит как простое число в том смысле, что оно удовлетворяет критерию Эйлера (2) для определенного числа a) – в этом случае a называется *EL-числом* (Euler liar). Ошибка теста Соловея–Штрассена, т. е. вероятность признать составное число n простым, не превышает $(1/2)^t$, где t – параметр, задающий число циклов в тесте.

В настоящее время тест Соловея–Штрассена вытеснен тестом Миллера–Рабина[15], который использует усовершенствованный критерий принятия решения, но при этом в нем также используется функция Эйлера $\varphi(n)$. Ошибка теста Миллера–Рабина не превышает $(1/4)^t$ при прочих равных условиях. Тест Миллера–Рабина в свою очередь используется при генерации простых чисел методом случайного поиска или при генерации сильных псевдопростых чисел по алгоритму Гордона.

Тесты на простоту широко используются при генерации параметров асимметричных криптосистем, а, как мы убедились, полученные Эйлером результаты имеют исключительно большое значение для построения алгоритмов тестирования чисел на простоту.

2. *Вычислительно сложные задачи теории чисел.* Три важнейших направления работ Эйлера: доказательство теоремы (1), исследование свойств квадратичных вычетов, создание теории первообразных корней – оказались тесно связаны с тремя вычислительно сложными задачами теории чисел, которые теперь положены в основу наиболее употребительных асимметричных криптосистем, а именно: с задачей Райвеста–Шамира–Адлемана (RSA), задачей о квадратичных вычетах и задачей дискретного логарифмирования соответственно.

Задача RSA заключается в следующем: по заданному положительному целому числу n, являющемуся произведением двух больших простых чисел q и p, положительному целому числу e, такому, что $НОД(e, \varphi(n)) = 1$, и целому числу c найти число m, такое, что $m^e \equiv c \ (\mathrm{mod} n)$. Иными словами, задача RSA заключается в нахождении корня степени e по модулю большого составного

числа n. Нахождение этого числа возможно путем применения расширенного алгоритма Евклида через нахождение числа d, такого, что $ed \equiv 1(\mathrm{mod}\varphi(n))$, где $\varphi(n) = (p-1)(q-1)$.

В силу этого задача RSA легко разрешима, если известно разложение n на простые сомножители, и требует факторизации числа, если это разложение неизвестно. Напомним, что все известные алгоритмы факторизации требуют сверхполиномиального времени, а потому задача RSA становится вычислительно сложной. Таким образом, в основе алгоритма решения задачи RSA лежит все та же теорема Эйлера (1).

Задача о квадратичных вычетах заключается в следующем: по данному нечетному составному числу n и числу $a \in J_n$, где J_n – множество всех $a \in Z_n^*$, для которых символ Якоби равен 1, решить, является или нет число a квадратичным вычетом по mod$n$: $a \stackrel{?}{\in} Q_n$. Напомним, что символ Якоби – это обобщение символа Лежандра для любых нечетных n, которые не обязательно являются простыми. Для $n \geq 3$, имеющего разложение на простые сомножители $n = p_1^{e_1}, p_2^{e_2} \ldots p_k^{e_k}$, он определяется так: $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \ldots \left(\frac{a}{p_k}\right)^{e_k}$.

В частном случае, когда n простое, он совпадает с символом Лежандра.

Решение задачи распознавания квадратичных вычетов возможно при известном разложении n на простые сомножители p и q, поскольку если $a \in J_n$, то $a \in Q_n$ тогда и только тогда, когда $\left(\frac{a}{p}\right) = 1$, т. е. в этом случае задача сводится к вычислению символа Якоби (символа Лежандра), для чего используется критерий Эйлера (2) и квадратичный закон взаимности (3).

Задача дискретного логарифмирования заключается в следующем: по заданному простому числу p, образующему элементу a мультипликативной группы Z_p^* и элементу $ß \in Z_p^*$ найти целое число x, $0 \leq x \leq p-2$, такое, что $a^x \equiv ß(\mathrm{mod}p)$. Задача дискретного логарифмирования алгоритмически неразрешима за полиномиальное время в группе Z_p^* и в подгруппах группы Z_p^*, поэтому она используется для построения однонаправленных функций в асимметричных криптосистемах.

С задачей дискретного логарифмирования тесно связана задача Диффи–Хеллмана: по заданному простому числу p, образующему элементу мультипликативной группы Z_p^* и элементам $a^a \mathrm{mod}p$, $a^b \mathrm{mod}p$ найти $a^{ab} \mathrm{mod}p$. Известно, что задача Диффи–Хеллмана не более сложна, чем задача дискретного логарифмирования,

но эквивалентность их пока не доказана. Пока эффективных способов решения задачи дискретного логарифмирования не найдено (за исключением особых случаев, которые мы здесь не обсуждаем), задача Диффи–Хеллмана также является вычислительно сложной. Напомним, что понятие первообразного корня впервые ввел Эйлер, он же исследовал его свойства, а именно на этом материале основано определение функции дискретного логарифмирования.

Таким образом, мы убедились, что сформулированные Эйлером результаты являются той теоретической платформой, которая делает возможным практическое использование вычислительно сложных задач и основанных на них однонаправленных функций в криптографии.

3. *Криптосистемы, основанные на вычислительно сложных задачах*. Задача RSA является основой стойкости схемы открытого шифрования RSA и схемы цифровой подписи RSA. На задаче о квадратичных вычетах базируется стойкость таких криптосхем, как вероятностная схема открытого шифрования Гольдвассера–Микали (Goldwasser–Micali) и псевдослучайного генератора BBS (Blum–Blum–Shub), схемы открытого шифрования Пайе (Paillier). На задаче дискретного логарифмирования основана схема открытого шифрования Эль-Гамаля, схема цифровой подписи Эль-Гамаля и ее варианты: DSA (американский стандарт цифровой подписи) и ГОСТ Р 34.10-94 (первый отечественный стандарт цифровой подписи). Задача дискретного логарифмирования в последнее время все чаще стала использоваться не в теоретико-числовой формулировке, а применительно к группам точек эллиптических кривых. И хотя это уже совсем другой раздел математики, но идеология формулирования и использования этой задачи в криптографических применениях берет свое начало в классической задаче дискретного логарифмирования.

4. *Криптографические протоколы, в которых используются примитивы на основе рассмотренных вычислительно сложных задач*. Помимо использования в криптографических протоколах перечисленных выше готовых криптосхем, в качестве «строительных блоков» в них могут применяться отдельные конструкции, стойкость которых основана на тех же вычислительно сложных задачах.

Самый известный пример – протокол открытого распределения ключей Диффи–Хеллмана, а также многочисленные производные от него протоколы, например MTI, STS и др. Стойкость их

всех в конечном счете основана на задачах дискретного логарифмирования и Диффи–Хеллмана.

Менее известные примеры – протоколы доказательства с нулевым разглашением знания, которые могут использовать все три рассмотренные выше задачи. Так, к примеру, стойкость протокола аутентификации Шнорра с нулевым разглашением знания базируется на сложности решения задачи дискретного логарифмирования.

Совсем мало известные пока примеры протоколов с использованием таких задач – это протоколы дистанционного контроля целостности баз данных[16], в которых используется задача распознавания квадратичных вычетов.

Рассмотренных примеров вполне достаточно для того, чтобы сделать вывод о принципиальной значимости полученных Л. Эйлером результатов для современной криптологической науки. При всем этом история распорядилась таким образом, что важнейшие результаты, казавшиеся многим при жизни Эйлера некоей «игрой в числа», стали востребованы наукой и, более того, составили математическую основу асимметричной криптографии спустя двести лет после смерти Л. Эйлера.

5. Вклад Л. Эйлера в развитие математического образования в России

Как мы уже убедились, Л. Эйлер был величайшим ученым, homo universalis своего времени, который сумел охватить едва ли не все области современного ему математического и естественнонаучного знания. Но весьма значителен был и масштаб его учебно-методической работы, который базировался на опыте преподавания в академической гимназии при Академии наук в Петербурге и научного руководства своими учениками. Этой сфере деятельности Л. Эйлера также посвящена обширная литература, из которой мы выделим наиболее основательные работы Г.С. Поляковой[17]. Отмечая тот факт, что любые выводы и оценки вклада Л. Эйлера в эту область, в отличие от области «чистой» математики, будут заведомо субъективны, тезисно сформулируем наши выводы о значении деятельности Эйлера для развития математического образования в России.

1). Эйлер сформулировал *фундаментальные методические идеи* в области математического образования. Основные из них таковы.

Во-первых, это *четкая структуризация и комплексирование математических дисциплин* в образовательном процессе. Эйлер считал обязательным изучение арифметики, геометрии, тригонометрии и «учения о шаре» – комбинации современных стереометрии и геодезии. Разумеется, этот комплекс лишь приблизительно соответствует содержанию современных дисциплин с теми же названиями. Однако не будем забывать, что Эйлер – первопроходец в этой области: до него в России по большому счету не было регулярного математического образования, а в учебных заведениях Западной Европы эти дисциплины имели далеко не первостепенное значение. Образованию была присуща многопредметность и как следствие фрагментарность получаемых знаний и навыков, разнесенность их по разным дисциплинам и этапам обучения.

Во-вторых, *соответствие содержания и процесса преподавания дисциплин основным дидактическим принципам*: системности, научности, доступности. Пример такого одновременного присутствия и разумного сочетания всех этих принципов подавал сам Эйлер, как было показано ранее на примере «Писем к немецкой принцессе...».

В-третьих, *поддержание системы математического образования в актуальном состоянии*. Содержание образования должно откликаться на ход передовой научной мысли, на полученные учеными новые важнейшие результаты. Научный поиск есть непосредственное продолжение «организованного» образования, переходящее преимущественно в форму самообразования. Эйлер прекрасно понимал эти истины и демонстрировал их на своем личном примере. В этом смысле Л. Эйлер был одним из первых ученых, которые осознали, что система образования, в частности математического, должна быть нацелена не просто на подготовку грамотных или «мудрых» людей, но на воспроизводство профессионального слоя ученых. Преподавание математических дисциплин на высоком профессиональном уровне служит необходимым условием достижения этой цели.

В-четвертых, *преемственность образования*: содержание образования низшей ступени должно служить базисом высшей ступени, недопустимы разрывы в содержании или пропуски отдельных дисциплин.

2). Эйлер разработал содержательное наполнение комплекса учебных дисциплин, который лежит в основе среднего, а отчасти и высшего математического образования вплоть до настоящего времени. С этой целью Эйлер написал учебники: знаменитое двух-

томное «Руководство к арифметике для употребления в гимназии императорской Академии наук» и «Универсальную арифметику» (по сути учебник алгебры, значительно превосходивший потребности школьного образования того времени). Кроме того, ему приписывается незавершенная рукопись учебника тригонометрии, авторство которого, однако, достоверно не установлено. Эйлером написано множество учебников и учебных руководств по прикладным наукам, в которых активно используется математический аппарат.

3). Наконец, еще одна заслуга Эйлера (может быть, не столь заметная по сравнению с перечисленными выше, но весьма важная именно для образования) состоит в том, что он ввел многие математические символы и обозначения, которые сделали математику «внятной» и доступной для понимания широкому кругу учащихся. Так, например, Эйлер предложил известные всем обозначения тригонометрических функций *sin*, *cos*, *tg*, решил вопрос о знаках тригонометрических функций, ввел для них круг единичного радиуса, а для функций комплексного аргумента ввел обозначение мнимой единицы $i = \sqrt{-1}$, что существенно упростило многие формулы. Благодаря Эйлеру учебники математики и математическая литература во многом приобрели привычный для нас вид.

6. Наследие Л. Эйлера и русская математическая школа

Л. Эйлер создал свою научную и методическую школу в императорской Петербургской академии наук, которая была по существу первой в России профессиональной математической научной школой. Он не просто создал научную школу, но поставил ее на один уровень с передовыми научно-образовательными школами Европы. К школе Эйлера традиционно относят восьмерых его учеников[18]: М.Е. Головина, С.К. Котельникова, С.Я. Румовского, П.Б. Иноходцева, В.Л. Крафта, А.И. Лекселя, Н.И. Фусса и А. Эйлера. Впоследствии все они стали академиками, хотя и были учеными далеко не первой величины. Их научная деятельность в основном выражалась в завершении тех задач, которые не успел решить Эйлер, а главные их заслуги относятся к области учебно-методической работы. Как преподаватели, методисты и популяризаторы науки они были, безусловно, талантливы и значительно повлияли на дальнейшее развитие математики в России.

Однако наибольшее влияние на дальнейшее развитие математики в России оказали работы самого Эйлера, сохраненные

и опубликованные его научной школой. Выявлению многочисленных «нитей», которыми связаны последующие поколения математиков с идеями Эйлера[19], посвящена обширная литература, тем не менее вряд ли эту тему можно считать исчерпанной. Придерживаясь поставленной в статье задачи, отметим здесь только влияние Эйлера на русскую теоретико-числовую школу.

Прежде всего работы Эйлера оказали огромное влияние на деятельность В.Я. Буняковского, который не только развил многие положения Эйлера в области теории сравнений, разложения чисел на множители, приложения теории чисел к другим разделам математики и других разделов математики к теории чисел, доказал ряд высказанных им предположений, но и участвовал в издании и комментировании рукописей Эйлера.

Далее М.В. Остроградский, опираясь на работы Эйлера в области теории первообразных корней, завершил в 1836 г. составление «Таблицы первообразных корней для всех простых чисел <200».

Для П.Л. Чебышёва, который внес большой вклад в теорию сравнений и теорию решения неопределенных уравнений в целых числах, знакомство с теорией чисел также началось с работы по изданию «Собрания арифметических сочинений» Эйлера (совместно с Буняковским). Изучая и комментируя сочинения Эйлера, он пришел к значительным выводам о распределении простых чисел, об арифметических функциях простых чисел и квадратичных формах.

На работах Эйлера были воспитаны и ученики П.Л. Чебышёва, принадлежащие к Петербургской математической школе: А.Н. Коркин, Е.И. Золотарев, А.А. Марков, А.В. Васильев, Ю.В. Сохоцкий. Это примеры прямого влияния работ Эйлера на следующее за ним поколение российских математиков. Разумеется, чем дальше отстояла эпоха от века Эйлера, тем многочисленнее и разветвленнее становились прямые и косвенные пути воздействия его работ на ученых, методистов и преподавателей высшей школы. Достаточно сказать, что практически все российские и советские школьные учебники алгебры вплоть до учебника А.П. Киселёва, по которому училась бóльшая часть нынешнего поколения людей среднего и старшего возраста, строились по заложенной Л. Эйлером методической концепции. Таким образом, наследие Эйлера оказывало заметное воздействие на работы русских ученых-математиков в течение нескольких десятилетий, пока разрабатывались поставленные им научные проблемы, а по завершении этого этапа, после стабилизации соответствующей отрасли знания навсегда стало «ядром», фундаментом математического образования.

7. Изучение наследия Л. Эйлера в наши дни

Известное на сегодняшний день письменное наследие Эйлера составляет 866 работ, включая 12 однотомных книг, 8 многотомных изданий, а также обширные собрания его переписки с видными российскими и зарубежными учеными-современниками: Даниилом и Иоганном Бернулли, Христианом Гольдбахом, Ж.Л. де Лагранжем, К.Г. Разумовским, Г.Н. Тепловым, И.К. Веттштейном. В наши дни почти все работы Эйлера (96,3%) доступны в первоисточниках на специально созданном сайте в сети Интернет[20]. «Архив Эйлера» сопровождается достаточно полными историческими и научными комментариями.

В 2007 г. во всем мире широко отмечалось 300-летие со дня рождения Л. Эйлера. В Швейцарии, Германии и России – странах, с которыми была связана жизнь и деятельность Эйлера, – прошли юбилейные мероприятия.

В наше время, когда актуальность научных исследований Л. Эйлера сменилась осознанием их классичности, изучение наследия Л. Эйлера приобретает совершенно новое значение. Лучше всего, пожалуй, оно выражается девизом основанного в 2002 г. Международного Эйлеровского общества (Euler Society), провозглашенным на его сайте[21]: «Общество использует жизнь и работы Эйлера как фундамент для попыток выявить более глубокие взаимосвязи между математикой, механикой, астрономией и технологией, начиная с XVIII в. и вплоть до настоящего времени». Для современных ученых и преподавателей Эйлер стал эталоном настоящего ученого и методиста, а его жизнь – образцом беззаветного служения людям и науке.

Работы Эйлера по-прежнему сохраняют основополагающее значение для математического, естественно-научного и технического образования. По неофициальной статистике, которая передается из уст в уста и в наши дни преподавателями высшей школы, имя Леонарда Эйлера – самое часто встречающееся в вузовских учебниках среди всех имен ученых. Действительно, ни один учебник высшей алгебры, аналитической геометрии, дискретной математики, комбинаторики, физики, теоретической механики, кристаллографии, геодезии и картографии, не говоря уже об учебниках теории чисел или математического анализа, не обходится без упоминания имени Леонарда Эйлера в связи с тем или иным впервые полученным им фундаментальным научным результатом важнейшего значения.

В связи с этим сейчас, как и 200 с лишним лет назад, по-прежнему актуальны слова П.-С. Лапласа: “Lisez Euler, lisez Euler, c’est notre maître à tous” («Читайте Эйлера, читайте Эйлера: он общий учитель для всех нас»).

Заключение

Проведенное исследование позволяет сделать следующие основные выводы.

1. Леонард Эйлер, по праву называемый самым великим математиком XVIII столетия, внес колоссальный вклад в развитие «чистой» и прикладной математики, механики, физики и многих других отраслей естествознания и технических наук. В частности, он явился основателем тех разделов математики и открывателем тех фундаментальных закономерностей, которые спустя 200 лет составили математические основы асимметричной криптографии (криптографии с открытым ключом).

2. При исключительной значимости математического наследия Л. Эйлера в целом наиболее существенным его научным результатом, представляющим интерес для современной криптологии, явилась системная разработка проблем теории чисел, что сделало возможным формирование теоретической и методологической базы криптологии (тестирование чисел на простоту, теория сравнений, теория квадратичных вычетов, теория первообразных корней и др.) и прикладное использование этих результатов в криптосхемах и протоколах (формулировка вычислительно сложных задач и построение на их основе однонаправленных функций).

3. Наиболее существенное значение методической деятельности Л. Эйлера заключается в создании оригинальной концепции систематического математического образования и разработке содержательного наполнения основных школьных математических дисциплин, что во многом определило стратегию развития российского математического образования на этапе его становления и задало высокий стандарт качества традиционного отечественного образования.

4. Научные труды Л. Эйлера послужили мощным импульсом развития российской математической, и в особенности теоретико-числовой, школы. Влияние Л. Эйлера на русских математиков было как прямым – через учеников, последователей и издателей научных трудов, так и косвенным – посредством формулировки им в своих научных трудах целого комплекса нерешенных науч-

ных проблем и запечатленного в его научном наследии личного примера беззаветного служения науке и обществу.

5. Изучение основополагающих элементов научного наследия Л. Эйлера в наше время следует рассматривать как необходимую (или крайне желательную) составляющую школьной и вузовской математической подготовки. По специальностям, связанным с информационной безопасностью, математическое наследие Эйлера составляет фундамент теоретической подготовки, а широкому кругу обучаемых помогает формировать кругозор, развивать эрудицию и воспитывать высокую культуру мышления.

Искренне благодарю моего первого учителя криптографии и научного руководителя учебно-исследовательских работ Александра Алексеевича Варфоломеева, который сразу и на всю жизнь связал в моем сознании криптографию с именем великого Леонарда Эйлера.

Примечания

[1] См.: *Запечников С.В.* Из истории криптографии: тайнопись как явление древнерусского литературного языка (XII–XVII вв.) // Безопасность информационных технологий. 2011. № 2. С. 116–123.

[2] Цит. по: *Козлов В.В.* Эйлер и математические методы механики (к 300-летию со дня рождения Леонарда Эйлера) // Успехи математических наук. 2007. Т. 62. Вып. 4 (376). С. 4.

[3] См.: *Эйлер Л.* Письма к немецкой принцессе о разных физических и философских материях // Л. Эйлер; ред. П.В. Симонов [и др.]; подг. изд. М.А. Бобович [и др.]. СПб.: Наука, 2002. 720 с. (Серия «Классики науки»).

[4] Там же. С. 23.

[5] Там же. С. 39.

[6] Цит. по: *Андерсон Дж.* Дискретная математика и комбинаторика: пер. с англ. М.: Вильямс, 2004. С. 438.

[7] См., напр.: Г*неденко Б.В.* Очерки по истории математики в России / Предисл. и коммент. С.С. Демидова. 4-е изд. М.: Либроком, 2009. С. 72–83 (Физико-математическое наследие: математика (история математики)); *Ожигова Е.П.* Очерки по истории теории чисел в России / Отв. ред. А.В. Малышев. 3-е изд. М.: Едиториал УРСС, 2011. С. 15–56.

[8] *Козлов В.В.* Указ. соч. С. 4.

[9] Все формулы в статье приводятся в современных нам обозначениях. При этом следует помнить, что ученые XVIII в. пользовались другими, менее удобными

обозначениями или описывали свои результаты словами. В частности, обозначение сравнения ≡ ввел Гаусс в начале XIX в.

[10] Дальнейшая интерпретация результатов Эйлера, относящихся к квадратичным вычетам, дается по работе: *Ожигова Е.П.* Указ. соч. С. 34.

[11] Там же. С. 32–33.

[12] См.: *Нестеренко Ю.В.* Теория чисел: Учеб. для студ. высш. учеб. заведений / Ю.В. Нестеренко. М.: Академия, 2008. С. 53–54.

[13] *Menezes A.J.* Handbook of Applied Cryptography [Электронный ресурс] / A.J. Menezes, P.C. vanOorschot, S.A. Vanstone. P. 136–137. URL: www.cacr.math.uwaterloo.ca/hac (дата обращения: 01.02.2012).

[14] Ibid. P. 137–138.

[15] Ibid. P. 138–140.

[16] См.: Provable data possession at untrusted stores [Электронный ресурс] / G. Ateniese [at all]. URL: http://eprint.iacr.org/2007/202 (дата обращения: 01.02.2012).

[17] См.: *Полякова Г.С.* Леонард Эйлер и математическое образование в России. М.: КомКнига, 2007. 184 с.

[18] *Гнеденко Б.В.* Указ. соч. С. 83.

[19] См., напр.: История математики (с древнейших времен и до XIX в.): В 3 т. / Ред. А.П. Юшкевич. М.: Наука, 1970–1972. Т. 3: Математика XVIII столетия. 498 с.; *Ожигова Е.П.* Указ. соч.

[20] См.: сайт «Архив Эйлера». [Электронный ресурс] [М., 2012] URL: www.dartmouth.edu/~euler (дата обращения: 01.02.2012).

[21] См.: сайт Международного Эйлеровского общества. [Электронный ресурс] [М., 2012] URL: www.eulersociety.org (дата обращения: 01.02.2012).

Тема номера

Ю.С. Чемеркин

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ КАК ИНСТРУМЕНТ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Облачные технологии являются на сегодняшний день наиболее многообещающими за счет своей гибкости, эффективности и экономической выгоды, приводя к тому, что до сих пор имеют место быть диспуты на тему недостаточной защищенности со стороны данных технологий. Именно поэтому целесообразно оценить имеющиеся проблемы и охарактеризовать вероятное их влияние, чтобы иметь возможность оценить возможные пути решения возникающих проблем или снижения рисков при внедрении облачных технологий.

В статье рассмотрены проблемы юридических документов в отношении вопросов регулирования облачных вычислений, выявлены пробелы современного российского законодательства в данной области, а также проблемы правовой защиты конфиденциальной информации с применением данных технических решений. Проведен анализ документов, связанных с обработкой персональных данных.

Ключевые слова: UML персональные данные, облачные вычисления, Amazon Web Service (AWS), облачные инструменты защиты и обработки информации, конфиденциальная информация, трансграничная передача данных.

Облачные вычисления (англ. cloud computing) представляют собой модель обеспечения повсеместного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам), которые могут быть оперативно предоставлены и освобождены с мини-

мальными эксплуатационными затратами и/или обращениями к провайдеру. Облачные вычисления, как правило, обладают следующими функциональными характеристиками:

– самообслуживание по требованию (self service on demand), позволяющее потребителю определять и изменять вычислительные потребности без взаимодействия с представителем поставщика услуг;

– универсальный доступ по сети, позволяющий получать услуги по сети передачи данных вне зависимости от используемого терминального устройства;

– объединение ресурсов (resource pooling), позволяющее поставщику услуг объединять ресурсы для обслуживания большого числа потребителей в единый пул для динамического перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности;

– эластичность, позволяющая предоставлять услуги, расширять и сужать их спектр в любой момент времени без дополнительных издержек на взаимодействие с поставщиком;

– учет потребления, позволяющий унифицировать потребляемые ресурсы с использованием определенного уровня абстракции, например объем хранимых данных, пропускная способность, количество пользователей, количество транзакций.

На сегодняшний день существуют следующие модели развертывания.

Частное облако (private cloud) – инфраструктура, предназначенная для использования, как правило, одной организацией. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны, и она может физически существовать как внутри, так и вне юрисдикции владельца.

Публичное облако (public cloud) – инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций. Публичное облако физически существует в юрисдикции владельца – поставщика услуг.

Общественное облако (community cloud) – вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики и соответствия различным требованиям). Общественное облако может

находиться в совместной собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны, и она может физически существовать как внутри, так и вне юрисдикции владельца.

Гибридное облако (hybrid cloud) – это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений.

В данной статье будет рассматриваться AWS-решение от компании Amazon, далее именуемое AWS, или Amazon. Amazon Web Services (AWS) – инфраструктура Web Services платформы в облаке, представленная компанией Amazon в начале 2006 г. В данной инфраструктуре представлено много сервисов для предоставления различных услуг, таких как: хранение данных (файловый хостинг, распределенные хранилища данных), аренда виртуальных серверов, предоставление вычислительных мощностей и др.

Под конфиденциальной информацией понимается та информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, которая представляет собой коммерческую, служебную, личную тайну или иной вид тайн, исключая государственную тайну, охраняющиеся ее владельцем. Так как соблюдение конфиденциальности является обязательным при обработке информации с ограниченным доступом, защита строится с применением как технических, так и правовых мер[1] (ФЗ № 149, ст. 9) с целью предотвращения неправомерных действий по осуществлению доступа и/или передачи со стороны не имеющих права на доступ к информации лиц (уничтожение, модифицирование, блокирование, копирование, предоставление, распространение). Также, согласно букве закона, должно обеспечиваться своевременное обнаружение фактов несанкционированного доступа к информации, возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, и постоянный контроль обеспечения уровня защищенности информации. Необходимо отметить, что последним пунктом является возможность возникновения «ограничений использования определенных средств защиты информации» со стороны Федерального закона, что часто неверно трактуется как невозможность применения зарубежных несертифицированных средств защиты.

Для дальнейшего рассмотрения требуется привлечение документов, регулирующих возникающие при обработке персональных данных правовые отношения в соответствии с приложением УП РФ № 188[2]. Так, согласно ст. 19 ФЗ № 152 «О персональных данных» при обработке должны приниматься необходимые меры или обеспечиваться их принятие, состав которых устанавливается «федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий» и раскрыт в приказе Федеральной службы по техническому и экспортному контролю (ФСТЭК)[3]. Также в соответствии со ст. 18.1 и 22.1 данного ФЗ лицами, ответственными за организацию обработки персональных данных, являются оператор и назначаемое им ответственное за обработку лицо, что показывает возможность привлечения третьих лиц для обеспечения адекватного уровня защиты при обработке информации.

Ключевыми моментами приказа ФСТЭК, исключая ряд пунктов, не применимых в условиях облачной парадигмы, являются:

• реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

• ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

• разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

• регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

• резервирование технических средств, дублирование массивов и носителей информации;

• использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

• использование защищенных каналов связи;

• организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

• предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;

• межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

• обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

• анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

• защита информации при ее передаче по каналам связи;

• использование средств антивирусной защиты;

• централизованное управление системой защиты персональных данных информационной системы;

• использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей.

Данный список удобнее представить в следующем виде:

– обеспечение конфиденциальности с точки зрения ограничения по сферам использования по отношению к внутренним и внешним заказчикам;

– уведомление обо всех известных утечках, так как в противном случае это ставит под угрозу конфиденциальность и целостность данных;

– раскрытие в той или иной мере с учетом законодательства данных для судебных разбирательств с предварительным уведомлением заказчиков о факте по требованию правоохранительных органов;

– оказание услуг в области шифрования в отношении хранимых (например, отдельного сервиса криптоконтейнеров) и передаваемых данных;

– переносимость данных как возможность выгрузки данных для передачи через Интернет;

– защита прав субъектов персональных данных и трансграничная передача данных при обработке персональных данных, а также вопросы в отношении местоположения виртуальных хранилищ данных в виде списка стран и наличия инструментальных средств работы с ними.

Целью данной работы является анализ документов, регулирующих вопросы, связанные с обработкой конфиденциальной информации и персональных данных с использованием облачных решений.

Для достижения поставленной цели необходимо решение следующих задач: во-первых, оценка степени разрешимости данных вопросов с позиции законодательных документов, EULA-документов (End-user license agreement, лицензионное соглашение с конечным пользователем) и SLA-документов (Service-level agreement, соглашение об уровне услуг) и во-вторых, оценка степени необходимости вовлечения дополнительных технических решений для соответствия законодательно предъявляемым требованиям.

В данной работе планируется акцентировать внимание на анализе законодательных документов в большей степени, чем EULA-документов и SLA-документов.

Последовательное рассмотрение обозначенных задач предпочтительно начать с таких вопросов, как, например, разграничение данных и их раскрытие. Инструменты управления и вообще сама архитектура облачных вычислений представляют собой[4] пласт виртуализированных сущностей (сервер, дисковое хранилище и т. п.), которые по умолчанию являются приватными (закрытыми), в том числе и сущности, связанные с сетевой передачей данных; однако последние публичны (открыты), как правило, по 2–3 протоколам передачи данных, известных как HTTP, HTTPS и RDP. Для осуществления непосредственного доступа, как это сделано в AWS, требуется точно указание виртуального хранилища и разрешение политики безопасности. Политика безопасности позволяет организовывать контроль на любое возникающее событие из доступного множества так называемых API-функций. Поэтому случайное подключение к чужой сущности невозможно, да еще и в обход политик ИБ, даже в режиме «по умолчанию» (т. е. с отсутствием разрешительных настроек всех, кроме обладателя ресурса).

Вопрос раскрытия данных в отношении третьих лиц в рекламных или иных целях должен заранее оговариваться и регламентироваться, ровно так же как и сроки использования информации. Очевидно, что рассматриваемые случаи при возникновении судебного процесса явно различаются между собой, но в общем виде могут быть сведены к двум различным вариантам развития событий, первым из которых является судебная повестка, адресованная

непосредственно лицу, чьи данные планируется раскрыть. Здесь требование раскрытия будет обязательным, однако существуют отдельные случаи, при которых поставщику услуг запрещается оповещать лицо о самом факте; обычно этот список законодательно оговорен в отношении представителей правоохранительных органов. Второй вариант развития событий – это случай, при котором повестка адресована другому лицу, и оповещения о факте раскрытия данных может и не быть. Так как судебные трактовки заранее не могут быть известны или недостаточно конкретны, достаточным решением будет выглядеть применение средств шифрования данных, в том числе и собственных (или сторонних, но отличающихся от встроенных). Таким образом, повестка будет требовать, чтобы облачный провайдер предоставил суду данные и доступ к ним, но у провайдера не будет ключей доступа к ним. В связи с этим суд должен будет отправить соответствующую повестку, что является вполне сопоставимым контролем над собственными данными в облачной среде, вне зависимости от типов последних.

Так, например, сервис Amazon S3[5], представляющий собой виртуальное дисковое хранилище, позволяет включать так называемое серверное шифрование, т. е. шифрование со стороны сервера в отношении каждого файла. При этом никто не запрещает загружать объекты, зашифрованные с использованием сертифицированных крипторешений или целиком криптоконтейнеры. Также присутствует возможность осуществлять шифрование виртуальных сущностей EC2 целиком, использовать ключи шифрования или хотя бы пароль для получения доступа к системе. Таким образом, рассматриваемая задача оказания услуг по шифрованию вполне разрешима уже с использованием предлагаемых облачным провайдером решений для хранения.

Рассмотрение вопроса касательно передачи выглядит аналогичным образом. Amazon по умолчанию использует SSL (Secure Sockets Layer, уровень защищенных сокетов; криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером) для передачи данных между своими сервисами. Возможна разработка приложений, использующих свои собственные механизмы передачи данных поверх https-протокола, либо же встраиваемых на уровне протокола, так как присутствует возможность спроектировать всю виртуальную архитектуру, включая внутренний DNS-сервер, с учетом требуемой специфики. Однако документация AWS четко разграничивает

(что удобно в контексте защиты и обработки различных типов данных) сферу применения своего набора решений, поэтому не рекомендуется использовать AWS EC2, которое представляет собой, упрощая, виртуальный сервер типа Windows Server для хранения и шифрования данных с учетом AWS-рекомендаций. Для разрешения этой проблемы применяется решение Amazon S3, тогда как вопросы передачи данных между различными сервисами, как внутри AWS, так и за ее пределами, решаются созданием и использованием облачных программ.

Вопросы, связанные с переносимостью (выгрузкой) данных решаются либо штатными средствами в штатном режиме, либо разработкой приложений, учитывающих конкретную специфику задач. Например, известный агрегатор облачных хранилищ SMEStorage позволяет автоматически выбирать хранилище для резервирования информации с конкретной виртуальной сущностью другого облака и автоматизировать процесс резервирования данных. Это также является решением вопросов компрометации, так как при возникновении последней и успешности определения вектора атаки с последующей временной оценкой случившегося процесс нескомпрометированной сущности будет занимать меньше 2–3 минут, что представляет собой самое минимальное время простоя. Однако надо отметить, что при этом будет иметь место финансовый вопрос, так как все облачные решения спроектированы так, что выгрузка данных обходится дороже, чем загрузка, а количество обращений к ресурсам тоже лимитировано в отношении тарифной сетки.

Дополнительным интересным аспектом является соблюдение требования удаления хранимой информации; в рамках возможностей AWS есть возможность задать автоматический предел хранения объекта, по истечению которого он становится недоступным. Учитывая понятие виртуализации с архитектурной стороны вопроса, можно провести аналогию с «драйвером дефрагментации», так как «свободное» место учитывается при выделении другого объекта в региональных рамках расположения серверов и затирается при создании новой виртуальной сущности. Здесь уместна некая аналогия с форматированием жесткого/логического диска, которым в данном случае является виртуальная сущность, приводящим к конечному виду (формату) для использования клиентом. Таким образом, обеспечивается право субъекта по ст. 14 ч. 1 ФЗ № 152 в отношении уничтожения данных[6]. Иногда действительно существуют некоторые проблемы с обеспе-

чением требования удаления персональных данных об отдельном субъекте отношений. Наглядно это проявляется в финансовом секторе, когда для сохранения отчетности, порой помещенной в архив, необходимо оставить информацию о субъекте. Однако данная проблема не является проблемой именно облачных вычислений, а является непосредственно недоработкой ФЗ № 152 «О персональных данных» в отношении временны́х рамок обработки информации.

На первый взгляд облачные вычисления ставят под сомнение возможность обработки данных за рубежом. Как известно, хранение уже является формой обработки. Согласно ст. 3 ФЗ № 152 «оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных», а обработчик (в том числе и инструментальный) – это облачный провайдер и/или непосредственно его решения по обработке информации в зависимости от того, кто является конечным лицом, осуществляющим обработку информации. Так, например, решение Microsoft Office 365 (онлайн-сервис от Microsoft, предлагаемый в аренду по типу SaaS) может быть предоставлено на территории России не непосредственно Microsoft, а иным представителем, например СКБ Контур. Если рассматривать прямой контакт с облачным провайдером, то возникают только два субъекта отношений с их договорными обязательствами. В случае прочих представителей или партнеров облачных провайдеров, предоставляющих свои ресурсы (например, в AWS предоставление ресурсов разрешено и технически легко реализуемо в отношении любого клиента), их количество увеличивается, но в договорные обязательства все также включены два субъекта со следующими поправками: рекомендуется оговаривание степени ответственности со стороны партнера, а также предоставление партнером информации о степени ответственности облачного провайдера в том случае, когда партнер напрямую не несет ответственности в отношении ряда пунктов договорных обязательств. Например, предоставление партнером своих ресурсов не привносит ответственности за их недоступность, если это произошло по вине Amazon по причине сбоя.

Требования ФЗ № 152 применяются как к официальным лицам, занимающимся обработкой информации, так и к лицам, непосредственно осуществляющим обработку по поручению оператора. Таким лицом будет являться облачный оператор и/или его

партнер, который также обязан обеспечить конфиденциальность данных в соответствии со ст. 6 и 7 ФЗ № 152. При этом обработчик не обязан получать согласие на обработку, хотя отметка о последнем должна присутствовать в договорных документах между заказчиком и оператором (ч. 4 ст. 9 ФЗ № 152); при этом третье лицо (как непосредственный обработчик данных) несет ответственность перед оператором, который поручил обработку. Примером являются договорные обязательства между клиентом и оператором сотовой связи T-Mobile, в которых указано, что провайдер использует технические средства, поставляемые компанией Carrier IQ для целей обеспечения услуги поддержки работоспособности своих сервисов и быстрого реагирования на возникающие инциденты. При этом данное техническое решение может собирать чувствительную информацию для перечисленных целей.

В соответствии со ст. 14 ФЗ № 152 «субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 настоящей статьи...». В качестве примера соответствий данным требованиям можно привести выборку из EULA- и SLA- документов сервиса Amazon, в которых говорится, что «компания Amazon не раскрывает информации о том, где физически располагаются их центры обработки данных; она просто декларирует, что каждый из центров размещается в ничем не примечательном здании с охраной периметра по типу армейской. Даже если мы знаем, что некий сервер базы данных находится в зоне доступности us-east-1a, мы все равно не знаем, ни где располагаются центры обработки данных, формирующие эту зону, ни даже какую из трех зон доступности на восточном побережье США представляет зона доступности us-east-1 a». Виртуализация сама по себе подчеркивает невозможность определения географического местонахождения пользовательских данных. Во-первых, данные хранятся в области, зарезервированной за пользователем. Во-вторых, данная область является эластичной, т. е. для нее со стороны пользовательских сценариев нет ограничений на размер данных, точнее данный размер автоматически растет с учетом изменения требований к ресурсам. В-третьих, данные хранятся с учетом архитектуры Amazon S3 избыточно, т. е. каждый файл представим, например, 12 частями,

из которых 8 являются значащими. Данная избыточность, как правило, позволяет исправлять ошибки в блоках данных. Таким образом, при работе с данными получение доступа (непосредственное) к «сырым» данным не приводит к получению данных на логическом (верхнем) уровне, чтобы последние представляли собой осмысленный документ, файл (зашифрованный или нет). AWS-инструменты позволяют в отношении своих ресурсов осуществлять непосредственно выбор географического местоположения виртуальных сущностей в пределах списка стран, где физически расположены их серверы. Это США, Ирландия, недавно в этот список был добавлен азиатский географический регион. Как известно, законодательство Евросоюза позволяет осуществлять обмен персональными данными не только со странами ЕС, но и со странами, которые обеспечили так называемый «адекватный уровень защиты персональных данных»[7]. К таким странам относятся следующие: Австрия, Андорра, Бельгия, Болгария, Дания, Великобритания, Венгрия, Германия, Греция, Израиль, Ирландия, Исландия, Испания, Италия, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словакия, Словения, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония. Одной из стран является Ирландия, которая входит в список стран, ратифицировавших Европейскую конвенцию по защите физических лиц при автоматизированной обработке персональных данных[8] и входит в список AWS-стран, где физически располагаются виртуальные сущности. Ратификация странами ЕС акцентирует для каждой из них запрещение накладывать дополнительные ограничения на передачу данных, если это не требуется для обеспечения конституционного строя, а также в отношении требований сертифицированных средств по причине того, что каждая страна-участница выполняет рекомендации по защите, принятые у нее, которые в свою очередь являются достаточными.

В ходе данной работы были решены следующие поставленные задачи:

– проведен анализ правовых документов по вопросам регулирования процессов обработки конфиденциальной информации и персональных данных;

– выявлена степень вовлеченности технических решений (в особенности интегрированных) для выполнения законодательных требований по применению инструментов обработки, в том числе сертифицированных средств.

На основании полученных результатов были сделаны следующие выводы:

1) рассмотренные правовые документы не предъявляют каких-либо существенных требований к ПО; непосредственные требования в части ПО, предусмотренные Приказом ФСТЭК России, имеют отношение исключительно к технологической платформе, а не к ее конфигурации;

2) существующие решения, построенные на основе облачных вычислений, могут быть использованы для целей обработки конфиденциальной информации и персональных данных;

3) облачные решения предоставляют как встроенные механизмы, позволяющие обеспечить соответствующую степень защиты информации, так и позволяют встраивать собственные сертифицированные механизмы;

4) несмотря на возможность расположения данных вне пределов РФ, ФЗ № 152 прямо предусматривает возможность трансграничной передачи данных согласно ст. 12;

5) отсутствие необходимости применения отечественных сертифицированных средств для целей обработки информации, не связанных с государственной тайной, с учетом ратифицированной европейской конвенции.

Представленные в данной работе наработки могут использоваться как для построения корректных регламентов ИБ, модели безопасности, политик безопасности и рабочих инструкций при эксплуатации облачных вычислений, так и для построения дополнительных инструментов обработки.

Целью дальнейшего исследования является более детальная проработка EULA-документов и SLA-документов различных облачных провайдеров для оценки степени сложности построения гибридных решений с применением решений от различных провайдеров.

Примечания

[1] См.: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 06.04.2011) // Российская газета. 2006. 29.07. № 165.

[2] См.: Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.) // Собрание законодательства РФ. 26.09.2005. № 39. Ст. 3925.

[3] См.: Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» // Российская газета. 2010. 05.03. № 46.

[4] См.: Архитектура облачных решений AWS. [Электронный ресурс] [М., 2012].URL: http://aws.amazon.com/documentation/ (дата обращения: 05.02.2012).

[5] См.: *Чемеркин Ю.С.* Проблемы новых парадигм и необходимости новых подходов к управлению облачными ресурсами // Информационная безопасность. 2012. № 1.

[6] См.: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных».

[7] См.: Письмо Министерства связи и массовых коммуникаций РФ от 13 мая 2009 г. № ДС-П11-2502 «Об осуществлении трансграничной передачи персональных данных». [Электронный ресурс] М., 2012.URL: http:// www.businesspravo.ru/ Docum/DocumShow_DocumID_153827.html (дата обращения: 05.02.2012)

[8] См.: Европейская конвенция по защите физических лиц при автоматизированной обработке персональных данных. 1981. [Электронный ресурс] // Сайт Роскомнадзора. [М., 2012].URL: http://64.rsoc.ru/law/p1262/p8861/ (дата обращения: 05.02.2012).

Е.П. Афанасьев

ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ПРИМЕНЕНИЯ ДОКУМЕНТО-ОРИЕНТИРОВАННЫХ ТЕХНОЛОГИЙ (на примере системы «Электронное правительство»)

Цель данной статьи – рассмотрение теоретических и практических вопросов защиты информации в условиях применения документоориентированных технологий на примере системы «Электронное правительство».

В ходе работы автором обозначены существующие проблемы системы электронного правительства, в частности рассмотрены слабые места подсистемы информационной безопасности: проанализированы возможные риски, существующие угрозы, обозначены каналы утечки информации. Также дается понятие существующих в системе «Электронное правительство» решений, касающихся защиты информации (инфраструктурные, аутентификационные, система защиты закрытых ключей). Кроме того, даны конкретные рекомендации по улучшению методов по защите информации в системе «Электронное правительство». Рекомендации касаются в первую очередь организационных методов.

Ключевые слова: электронный документооборот, документоориентированные технологии, электронное правительство, подсистема обеспечения информационной безопасности.

В последние годы руководство России придает большое значение внедрению электронных технологий в различные сферы жизни. Одно из приоритетных направлений внедрения информационно-коммуникационных технологий – создание «электронного правительства», т. е. использование информационных технологий в работе государственного аппарата.

Условием бесперебойного функционирования системы электронного правительства является обеспечение необходимого и до-

статочного уровня информационной безопасности его компонентов. Выявление угроз информационной безопасности, обеспечение надежного противостояния, ликвидация неблагоприятных последствий нарушений защиты, регулярная оценка защищенности компонентов инфраструктуры, выявление новых угроз и своевременная модернизация систем защиты реализуются с помощью системы обеспечения информационной безопасности инфраструктуры электронного правительства.

Использование информационных систем (документоориентированных технологий) порождает риски. Риск можно рассматривать как получение непредвиденных или не ожидаемых в данном конкретном случае негативных результатов (по закону «О техническом регулировании»[1] «риск – вероятность причинения вреда»).

Все риски можно разделить на:

– информационные, не порождающие правовых и материальных (финансовых) последствий;

– бизнес-риски – порождающие правовые и/или материальные последствия или последствия, которые в конечном счете будут сведены к правовым и материальным.

Возможность «потери» юридической значимости электронных данных – риск, который может существенно повлиять на все результаты применения информационной системы (ИС).

Однако нельзя преуменьшать опасность информационных рисков. Возможность оценки рисков позволяет определить степень доверия к информации, содержащейся в системе. Но это обычно соблюдение формальной стороны вопроса – обеспечения юридической значимости документооборота. По сути это соблюдение формы.

Исходя из разделения документа на форму и содержание, можно также подразделять и риски на нарушение формы (риск искажения заложенной технологии обработки информации) и нарушение содержания (риск искажения смысла применения системы, когда все технологические нюансы соблюдены, но результат не тот, которого ожидали).

Типовыми источниками угроз можно назвать следующие:

– сознательные действия по вскрытию средств защиты;

– ошибки персонала;

– сознательные действия разработчиков («логические бомбы», backdoors и т. п.);

– ошибки и сбои информационных систем;

– выход из строя частей аппаратных комплексов;

– влияние внешних техногенных факторов.

В связи с тем что юридические документы переложены в электронный вид, возникает проблема защиты этих документов от искажения, утраты и т. п.

Средства защиты обычного документа не зависят от содержания, так же как содержание не влияет на используемые средства защиты. Защита носителя – печать, подпись, бланк, спецбумага, водяные знаки, вкрапления и др. Защита содержания носителем – невозможность исправления, целостность носителя (контроль полноты содержания). Проверка подлинности документа осуществляется контролем защитных средств носителя (сверка с эталоном) и отсутствием нарушений целостности носителя.

Защита электронного документа – это защита процессов: защита содержания как упорядоченности, защита технологий, инвариантных к защищаемой информации, и очень редко защита конкретного носителя и запрет копирования. Определенной, особенностью защиты электронного документа является прямая зависимость «маркера» защиты от содержания (ЭЦП одного лица меняется от документа к документу).

В результате можно сделать следующий вывод – различия в защите электронного и аналогового документа обусловлены базовыми различиями аналогового и электронного документа (форма и содержание, носитель, расположение, методы защиты).

Защита информации используется в системах документооборота для снижения уровня угроз и сокращения перечня возможных угроз. Речь идет об угрозах всех уровней, и прежде всего не случайных (типа отказа техники), а типовых.

Все угрозы с точки зрения системы документооборота (уровень абстракции – логически связанные и законченные для определенного этапа обработки электронные данные или документы) можно разделить на четыре типа:

– угрозы по отношению к соблюдению конфиденциальности информации;

– угрозы по отношению к соблюдению целостности информации, в том числе соблюдению целостности документа;

– угрозы по отношению к соблюдению технологии обработки (в том числе соблюдению условий юридической значимости действий);

– угрозы отказа в обслуживании[2].

Основными техническими и технологическими методами защиты являются следующие:

– шифрование (секретность, целостность);

– хэш-функции, контрольные суммы, помехоустойчивое кодирование (целостность);

– средства идентификации и аутентификации (в том числе аппаратные, биометрические);

– реализация моделей управления доступом: мандатная и дискреционная;

– сертификация;

– использование аналогов собственноручной подписи (прежде всего ЭЦП);

– протоколирование действий (пользователей и автоматических процессов).

Как основное средство для проверки подлинности документа, составленного в электронном виде, используется электронная цифровая подпись (ЭЦП), о которой говорится в Федеральном законе от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»[3]. С 01.07.2012 этот закон утрачивает силу в связи с принятием Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»[4].

Принадлежность секретного ключа электронной подписи конкретному лицу удостоверяется сертификатом. В сертификате, кроме всего прочего, указано, какие виды документов может подписывать владелец данной электронной подписи. Каждый сотрудник организации может иметь один или несколько сертификатов, которые удостоверяют и ограничивают его полномочия.

В состав системы обеспечения информационной безопасности инфраструктуры электронного правительства входят следующие подсистемы обеспечения информационной безопасности (ПОИБ):

– подсистема обеспечения информационной безопасности сети удостоверяющих центров;

– подсистема обеспечения информационной безопасности информационно-платежных шлюзов;

– подсистема обеспечения информационной безопасности прочих инфраструктурных информационных систем электронного правительства;

– подсистема обеспечения информационной безопасности иных информационных систем электронного правительства.

В системе «Электронное правительство» обрабатывается общедоступная информация и информация ограниченного доступа (персональные данные), не содержащие сведения, составляющие государственную тайну.

Работы по обеспечению безопасности информации являются неотъемлемой частью работ по созданию ИС и осуществляются в виде создания подсистем обеспечения информационной безопасности в составе каждой ИС в соответствии с принципом, закрепленном в концепции информационной безопасности для каждой ИС.

Для обеспечения защиты информации при ее обработке в ИС, реализуемых в рамках создаваемых подсистем обеспечения информационной безопасности, применяются следующие мероприятия:

– защита от несанкционированного доступа к информации, конфиденциальность и целостность информации;

– защита информации при межсетевом взаимодействии между ИС;

– защита информации от вредоносного воздействия компьютерных вирусов (антивирусная защита);

– обнаружение компьютерных атак;

– защита информации от утечки по техническим каналам;

– резервное копирование и восстановление информации.

Реализация мероприятий по защите информации обеспечивается комплексом средств защиты информации в составе ПОИБ. Типовой состав комплексной системы защиты информации состоит из следующих основных средств:

– защита информации от несанкционированного доступа;

– межсетевое экранирование;

– обнаружение сетевых атак;

– анализ защищенности;

– криптографическая защита информации, передаваемой по каналам связи;

– антивирусная защита;

– усиленная аутентификация при удаленном доступе к ресурсам ИС;

– защита информации от утечки по техническим каналам.

Выбор и применение средств защиты, используемых для защиты информации в ИС, осуществляется в соответствии с действующими требованиями, в том числе нормативных правовых актов ФСБ России и ФСТЭК России.

При организации системы «Электронное правительство» необходимо использовать механизмы, обеспечивающие:

– контроль целостности используемого программного обеспечения;

– регистрацию событий в информационных системах;
– криптографическую защиту;
– межсетевое экранирование;
– виртуальные частные сети;
– антивирусную защиту;
– аудит информационной безопасности.

Рассмотрим некоторые аспекты защиты системы «Электронное правительство».

Аутентификация пользователей. Однозначная идентификация возможна только с помощью аутентификации. Аутентификация – это подтверждение подлинности идентификатора, производимое, как правило, с помощью криптографических преобразований. Строгая аутентификация позволяет не только разделить, но и персонифицировать доступ, т. е. сделать всех пользователей, работающих, например, с персональными данными, персонально ответственными за все их действия с этими данными. Современным подходом для организации персонифицированного доступа является применение решений на базе Public key infrastructure (PKI), а механизмом аутентификации – процедура ЭЦП[5].

Инфраструктурные решения. Составными частями инфраструктуры обеспечения защиты системы электронного правительства являются:

инфраструктура электронных баз данных документов (реестров, регистров, кадастров), принадлежащих разным ведомствам;

инфраструктура ЭЦП, включающая уполномоченные удостоверяющие центры, входящие в единую систему на базе развитой инфраструктуры открытых ключей – PKI. Архитектура национальной системы PKI пока окончательно не утверждена, но все понимают, что существующие ведомственные «островки доверия» необходимо связать в единую систему;

инфраструктура доверенных сервисов, таких как доверенная третья сторона, инфраструктура доверенного времени (на основе доверенного источника времени) для проставления временных меток, прилагаемых к электронному документу: инфраструктура удостоверения места издания документа (сделки, контракта, договора, соглашения) двумя или более сторонами на основе доверенной третьей стороны;

инфраструктура электронных реестров участников информационного взаимодействия для подтверждения их правового статуса, правомочий, полномочий и права подписи.

Управление закрытыми ключами. Согласно п. 1 ст. 12 ФЗ № 1 «Об электронной цифровой подписи»[6] задача хранения закрытого ключа лежит на его владельце. У неподготовленного пользователя могут возникнуть проблемы с самостоятельным обеспечением безопасности своего закрытого ключа.

В нынешнем правовом поле для придания юридической значимости электронному документу имеется непростой, но уже хорошо известный алгоритм, включающий в себя ряд технологических, правовых и организационных мер. Так, при создании и использовании ключей ЭЦП необходимо использовать только сертифицированные средства ЭЦП и средства криптографической защиты информации. Для признания документов с ЭЦП равнозначными привычным бумажным документам необходимы также введение понятия аналога собственноручной подписи и создание регламента использования ЭЦП в каждой системе электронного документооборота (СЭД) или заключение соглашения сторон о применении ЭЦП в СЭД[7].

Можно выделить ряд проблем защиты системы электронного правительства. В первую очередь это несовершенство нормативно-правовой базы, в том числе в области законодательства, регулирующего электронный документооборот; разнообразие технических решений, входящих в систему «Электронное правительство»; большое количество передаваемой, обрабатываемой и хранимой информации и персональных данных.

В результате исследования можно дать следующие рекомендации по применению организационных методов защиты информации в условиях развития системы электронного правительства.

1. Чтобы электронное правительство начало эффективно действовать, нужно принять множество нормативных актов. То есть необходимо совершенствовать законодательство по следующим направлениям:

– четко разграничить полномочия всех органов власти в части создания и функционирования системы «Электронное правительство»;

– выработать единую методологию создания и функционирования системы электронного правительства во всех органах власти;

– согласовать положения федеральных, региональных и муниципальных нормативных актов по вопросам системы электронного правительства и устранить противоречия;

– разработать единые требования к функционалу системы с возможностью добавления дополнительных функций для каждого органа власти.

2. Необходимо разработать единую методику оценки угроз для объектов информатизации, входящих в электронное правительство.

Поскольку разные органы власти находятся на различных стадиях информатизации, то на начальном этапе система информационной безопасности должна строиться для каждого органа автономно, но обязательно на основе единых принципов и единой архитектуры, чтобы обеспечить согласованную работу в дальнейшем.

3. Необходимо выработать единые требования к защите информации во всех элементах системы электронного правительства, в частности:

– гарантировать соблюдение требований действующего законодательства и нормативных актов при создании и функционировании системы «Электронное правительство»;

– обеспечить наличие средств защиты обрабатываемой информации, позволяющих однозначно идентифицировать этап документооборота и ответственного за этот этап;

– предоставить возможность выделения формальных признаков юридически значимой информации;

– гарантировать защиту персональных данных участников системы электронного правительства;

– минимизировать возможность нанесения вреда одним участником системы другому;

– обеспечить возможности четкого разграничения полномочий участников системы и их ролей.

Основным принципом создания эффективной системы защиты электронного правительства является следующий: ни один из участников системы не должен иметь возможности нанести вред другому участнику, попытки нанесения вреда должны контролироваться и сообщаться тому, кому наносится вред (также добавляется контроль действий со стороны администратора).

В заключение необходимо отметить, что эффективная система защиты электронного правительства должна интегрировать разнородные средства защиты информации, необходимые для нейтрализации угроз безопасности всех ее компонентов, в единую взаимосвязанную среду, обеспечивающую выполнение целевых задач по информационной безопасности, вытекающих из моделей угроз и моделей нарушений, общесистемной политики безопасности и частных разделов политики безопасности.

Примечания

[1] См.: Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // Российская газета. 2002. № 245.

[2] См.: *Юрченко Т.В.* Информационные технологии в экономике. Решение экономических задач средствами MS EXCEL 2007 [Текст]: Учеб. пособие / Т.В. Юрченко; Нижегород. гос. архит.-строит. ун-т. Н. Новгород: ННГАСУ, 2010. 132 с.

[3] См.: Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» (ред. от 08.11.2007) // Российская газета. 2002. № 6.

[4] См.: Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета. 2011. № 75.

[5] См.: *Сабанов А.Г.* Некоторые аспекты защиты электронного документооборота [Электронный ресурс] [М.,2011] URL: http://ecm-journal.ru/print/Nekotoryeaspekty-zashhity-ehlektronnogo-dokumentooborota.aspx (дата обращения: 20.04.2011).

[6] См.: Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

[7] См.: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 06.04.2011) // Российская газета. 2006. № 165.

Г.А. Шевцова

РАЗВИТИЕ СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА И ИНФОРМАЦИОННАЯ ЗАЩИТА С ТОЧКИ ЗРЕНИЯ ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ

Информационные технологии неразрывно связаны с информационной системой, представляющей собой технологическую цепочку обработки сообщений. Преобразование сведений в сообщения осуществляется с использованием алгоритмов их кодирования в набор знаков сообщения, а сообщений – в сведения с использованием алгоритмов декодирования поступившего набора знаков. Обработка информации – преобразование одних электронных данных в другие, отличающиеся от исходных информационным содержанием, составом и формой. Результат преобразования представляет собой новый вид упорядоченности. Полученный электронный документ рассматривается в совокупности с электронной средой. Защита электронного документа включает в себя защиту технологии, т. е. непосредственно технологическую цепочку документооборота.

Ключевые слова: электронный документооборот, электронные данные, защита информационной системы, информационные технологии, кодирование, распространение информации.

Накопление, обработка и распространение информации – это задачи, которые стояли перед человечеством на всех этапах формирования общества. Причем они затрагивали как повседневную жизнь, так и развитие технологических процессов, являющихся неотъемлемой составляющей жизнедеятельности общества.

Информационная составляющая жизни сообщества людей – весьма сложное явление, единой трактовки которого в современной науке еще не сложилось. Обобщение практики законодательного регулирования отношений, связанных с информацией,

а также работ, выполненных в других областях науки, позволяет рассматривать информацию как результат отражения движения объектов материального мира в системах живой природы вообще и в организме человека в частности[1].

Информация существует в двух формах – в форме сведений и в форме сообщений.

Сведения представляют собой такую форму информации, в которой движение объектов реального мира посредством психической деятельности отражается в организме конкретного человека. Это отражение закрепляется в виде соответствующих биохимических преобразований морфологии мозга.

Конкретное содержание сведений определяется свойствами отражаемого объекта и особенностями отражения этих свойств в организме человека, а поведение – субъективной оценкой «перспективности» возможных вариантов удовлетворения его нужд, потребностей и интересов, осуществляемой человеком на основе накопленных сведений[2].

С точки зрения семантических свойств понятие «сведения» раскрывается как «знание, представление о чем-либо». Эти представления формируются на базе наблюдений и ощущений. Наблюдения и ощущения, возникающие в процессе отражения, трансформируются в сведения и опосредуются в «информационной» модели человека, которая помимо сведений, в том числе и в виде знаний, включает отношения между сведениями, субъективные оценки значимости сведений и отношений для осуществления конкретной деятельности, окрашивая их эмоционально.

Сведения выполняют несколько важных функций в жизнедеятельности человека:

– гносеологическую, связанную с познанием окружающего мира, включая формирование представлений об окружающей среде, ее свойствах, накопление знаний о закономерностях ее изменения и протекающих в ней процессах, а также с оценкой последствий изменения окружающей среды для существования человека;

– социальную, заключающуюся в формировании представлений о способах удовлетворения потребностей человека, о правилах поведения в обществе, взаимодействия с другими людьми, о нравственных ценностях в формировании «личностных» ценностей, материальных и духовных благ, а также допустимости использования известных средств для овладения ими;

– прагматическую, связанную с формированием, оценкой и выбором целей, достижение которых способствует удовлетворению

базовых и вторичных потребностей человека, его интересов, а также с деятельностью по достижению выбранных целей.

Как форма проявления информации сведения обладают рядом свойств, к числу наиболее важных следует отнести:

– духовность (нематериальность) – существование только в сознании человека и вследствие этого невозможность восприятия органами чувств;

– субъективность – зависимость количества и ценности сведений, получаемых субъектом, от его знаний, темперамента, нужд и потребностей;

– неуничтожаемость – невозможность физического уничтожения сведений, закрепленных в организме человека;

– динамичность – возможность изменения ценности запечатленных сведений, а также отношений, связывающих их с другими элементами «информационной» модели, под воздействием времени или других поступающих сведений.

Сообщения представляют собой такую форму существования информации, в которой сведения передаются от одного человека к другому и являются упорядоченной совокупностью знаков самой различной природы.

Понятие «сообщение» можно определить как «кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов (алфавита), образующих некоторую упорядоченную совокупность».

Воспринимая сообщение, психическая сфера человека устанавливает взаимосвязь между составляющим его набором знаков и известными человеку понятиями, а затем – с образами, эмоциями, ощущениями, оценками и связывающими их ассоциативными отношениями, т. е. преобразует сообщение в сведения.

Сообщение способно порождать в организме человека определенные сведения, и с этой точки зрения можно сказать, что оно содержит эти сведения.

Преобразование сведений в сообщения осуществляется с использованием алгоритмов их кодирования в набор знаков сообщения, а сообщений в сведения – с использованием алгоритмов декодирования поступившего набора знаков. Без алгоритмов кодирования и декодирования сообщение превращается просто в набор знаков.

Информация в форме сообщения обладает рядом свойств, к числу которых относятся:

– материальность – способность воздействовать на органы чувств;

– объективность – независимость набора знаков, составляющих сообщение, от получающего субъекта;

– отчуждаемость – возможность физического отделения набора знаков от субъектов, участвующих в передаче или обмене информацией;

– уничтожаемость – возможность физического уничтожения набора знаков, составляющих сообщение;

– статичность – независимость набора знаков, которые составляют сообщение, от времени, прошедшего с момента его создания;

– ограниченная воспроизводимость – возможность точного воспроизведения только после закрепления на том или ином носителе;

– копируемость – возможность создания сколь угодно большого числа копий сообщения, закрепленного на некотором носителе.

Нельзя преуменьшать значение информации в форме сведений. Именно в этой форме субъект как конечный получатель информации зафиксирует информацию в своем сознании. Однако для документооборота важно представление информации в форме сообщения. Именно эта форма позволяет рассматривать информацию как объект материального мира, придавать ей свойства документа и применять соответствующие понятия.

Сегодня информационный объект невозможно представить без информационных технологий, которые объединяются в широкий класс дисциплин и областей деятельности, относящихся к вопросам создания, сохранения, управления и обработки данных, в том числе с применением средств вычислительной техники. В последнее время под информационными технологиями чаще всего понимают компьютерные технологии. В частности, информационные технологии имеют дело с использованием компьютеров и программного обеспечения для создания, хранения, обработки, ограничения к передаче и получению информации. А если рассматривать еще шире, то информационные технологии – это комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы. Сами информационные технологии требуют сложной подготовки, больших первоначальных

затрат и наукоемкой техники. Их внедрение должно начинаться с создания материального обеспечения, моделирования, формирования информационных хранилищ для промежуточных данных и решений.

Можно выделить основные черты современных информационных технологий, важнейшими из которых являются:

• структурированность стандартов цифрового обмена данными алгоритмов;

• широкое использование компьютерного сохранения и предоставление информации в необходимом виде;

• передача информации посредством цифровых технологий на практически безграничные расстояния.

Информационные технологии неразрывно связаны с информационной системой, представляющей собой систему формирования, отправления, получения, хранения или иной обработки сообщений.

К основным требованиям, предъявляемым к информационной системе, используемой для обработки документов, относятся;

– обеспечение понятности документа (реализуется технологически через алгоритм преобразования информации, юридически – через введение требований к форме, доступной для понимания человека);

– обеспечение неизменности документа со временем (реализуется технологически через процедуры защиты от несанкционированного доступа и разграничения доступа к электронным архивам, резервное копирование информации, в том числе на автономные носители, юридически – через установление обязанности хранения электронного документа в течение срока, аналогичного для бумажных документов, а также требований к ведению электронных архивов);

– обеспечение возможностей воспроизведения документа с одинаковыми данными у каждой стороны (реализуется технологически через унификацию стандартов передачи данных, алгоритмы программного контроля и использование электронной цифровой подписи (ЭЦП), юридически – через установление юридических презумпций отправления и получения электронных документов, процедуры подтверждения получения электронных документов, а также обязательности контроля документа на предмет ошибок);

– обеспечения возможностей для удостоверения подлинности данных посредством подписи (технологически через ЭЦП, юридически – через установление критериев их надежности, связь юри-

дической силы электронных документов с подтверждением подлинности);

– обеспечение приемлемости формы документа для государственных органов и судов (технологически – через сертификацию технических средств, используемых для организации документооборота с госорганами, разработку госорганами форматов электронных документов; юридически – через право госорганов предписывать правила предоставления электронных документов, признание доказательственной силы электронных документов и установление специальных процессуальных норм).

Суть обработки информации – преобразование одних электронных данных в другие, отличающиеся от исходных информационным содержанием, составом, формой представления таким образом, что результат преобразования представляет собой новый вид упорядоченности. В результате обработки появляются логически законченные электронные данные, воспринимаемые системой. Для описания обработки информации необходима формализация общего информационного пространства и преобразующих воздействий с целью выделения логически законченных блоков информации и представления процесса как: исходные данные + преобразование = результат, или как F-преобразование (исходные данные) = результат. При этом необходимо выбирать необходимый (оптимальный) уровень детализации и абстрагироваться от незначащих (по сути обработки) характеристик электронных данных (например, размещения данных на оперативном запоминающемся устройстве, физического расположения файла данных на носителе и т. п.). В приложении к документообороту значимость характеристик и уровень абстракции определяются в отношении существенных элементов документа – реквизитов. Однако иногда необходимо учитывать некоторые показатели систем, относящиеся не к собственно документу, а к состоянию системы (например, получение документа информационной системой получателя документа: информационное наполнение документа не изменилось, но изменился его статус в рамках информационной системы).

Конечно, на сегодня без автоматизации процессов документирования, т. е. без автоматизированной обработки информации с использованием автоматизированных систем, невозможно представить себе работу ни одной структуры. Весь комплекс действий по получению из набора исходных данных требуемого результата может быть разделен на этапы, которые выполняют как сама система, так и вспомогательный персонал.

Этапы могут выделяться по различным принципам: территориальным, технологическим, юридическим и т. п. Один из важнейших принципов выделения этапа – наличие в процессе обработки человеческого фактора, т. е. наличие оператора, который влияет на процесс обработки информации.

Влияние человеческого фактора возможно при выполнении следующих действий:

• ввод информации;

• принятие решения о выборе одного из нескольких возможных алгоритмов обработки на текущем этапе;

• исполнение системой некоторых действий, не приводящих к обработке документа, но влияющих на состояние системы или статус электронных данных в реальном аналоговом мире (например, распечатка документа, создание дополнительной электронной копии и т. п.).

Важность этого критерия будет видна отчетливее при рассмотрении вопросов ответственности и юридической значимости информации. В любой информационной системе можно выделить этапы, реализующие полностью автоматические и «ручные» процессы. При разделении на эти этапы стоит обратиться к вопросу выбора целесообразного уровня детализации.

Без разделения общей информационной системы на этапы невозможно построение этой системы и формирование требований к ней. На каждом из этапов будут свои требования к информационно-технической базе и собственная политика безопасности.

В электронном документообороте, как и в обычном, можно выделить этапы «жизни» / «прохождения» (обработки) документа. Каждый из этапов зависит от тех действий, которые были совершены в отношении документа на предыдущих этапах. Детерминированную последовательность этапов обработки электронного документа называют технологической цепочкой. Состав технологической цепочки зависит от требуемой последовательности действий с документом. Наличие документа (или данных) на выходе одного звена (процесса) порождает в системе действия, связанные с активизацией процессов следующего звена цепочки. Собственно технологическая цепочка и реализует документооборот. Элементарным «звеном» цепочки является некоторый типовой этап обработки документа. Например, заполнение реквизита, форматирование, заверение и т. п. Именно реализация конкретной технологической цепочки обеспечивает подлинность и корректность документа. Для реализации «правильного» документооборота не-

обходимо обеспечение правильной работы каждого элементарного звена и обеспечение соблюдения последовательности звеньев[3].

В общем случае ответственность за обеспечение правильности документооборота, т. е. получение истинных результатов, несет как каждое отдельно взятое звено, так и система, обеспечивающая взаимодействие этих звеньев. Очевидно, что в больших системах, содержащих различные аппаратные и программные средства, которые обслуживает персонал, необходимо выделять зоны ответственности. В зону ответственности входит контроль за действиями, обеспечивающими обработку информации, входящими в область компетенции производящего эти действия[4].

Автоматизированная система не сможет оценить корректность действий оператора в целом, т. е. правилен ли смысл вводимого текста или это ложная информация. Система может только указать оператору на грамматические ошибки и отклонение от принципов работы с системой. Со своей стороны оператор не сможет проконтролировать корректность сохранения информации на носителе.

В общем случае под защитой информационной системы следует понимать защиту реализованной технологии обработки информации, т. е. реализованной технологической цепочки. С точки зрения взаимодействия электронного и аналогового миров (юридической значимости электронных данных) соблюдение технологии обработки информации является критерием значимости результатов обработки. С прикладной точки зрения необходимо обеспечить условия, при которых в процессе создания и обработки электронных документов (электронных данных) изоморфизм собственно преобразований и изоморфизм множества сигналов (нулей и единиц), маркированного как «информация», будут сохраняться. Существенно, что если каждое преобразование из множества применяемых в процессе обработки электронного документа сохраняет изоморфизм документа, то в силу свойства транзитивности сохраняет изоморфизм вся совокупность (технология) преобразований. Таким образом, электронный документ нельзя рассматривать в отрыве от электронной среды. Защита электронного документа должна включать в себя и защиту технологии – факторов, инвариантных «содержанию» электронного документа, не зависящих от него, т. е. непосредственно технологическую цепочку документооборота.

Примечания

[1] См.: *Ларин М.В.* Управление документацией в организациях. М.: Научная книга, 2002.

[2] См.: *Стрельцов А.А.* Правовое обеспечение информационной безопасности России: теоретические и методологические основы. Минск, 2005. 304 с.

[3] См.: *Березина Н.М., Лысенко Л.М., Воронцова Е.П.* Современное делопроизводство. 3-е изд. СПб: Питер, 2008.

[4] См.: Правовое обеспечение информационной безопасности / Под ред. С.Я. Казанцева. М.: Академия, 2007. 240 с.

С.А. Желтов

АДАПТАЦИЯ МЕТОДА ШЕРМАНА–ЛЕМАНА РЕШЕНИЯ ЗАДАЧИ ФАКТОРИЗАЦИИ К ВЫЧИСЛИТЕЛЬНОЙ АРХИТЕКТУРЕ CUDA

Статья посвящена некоторым аспектам организации параллельных вычислений и использования технологии GPGPU для решения задач факторизации целых чисел. Основные разделы посвящены обзору вычислительной архитектуры CUDA, ее особенностей и адаптации метода Шермана–Лемана к параллельным вычислениям на графических устройствах.

Ключевые слова: параллельные вычисления, факторизация целых чисел, архитектура CUDA.

К числу актуальных задач характеризуемых высокой вычислительной сложностью, относятся задачи, используемые в приложениях информационной безопасности (ИБ).

Задача факторизации целых чисел[1] лежит в основе целого ряда асимметричных криптографических систем, используемых в самых различных областях социально-экономической деятельности. Наиболее известной криптосистемой такого рода является система RSA[2], используемая для защиты программного обеспечения в схемах цифровой подписи, в открытой системе шифрования PGP и других системах шифрования, например в DarkCryptTC и формате xdc.

Формально задачу факторизации целых чисел можно сформулировать следующим образом: для заданного числа $n \in Z$ надо найти его разложение на простые множители $p_i \in N$, такие что $n = \prod_{i=1}^{l} p_i^{a_i}$, $a_i \in N$.

Задача относится к классу NP и на сегодняшний день не известны методы ее решения полиномиальной сложности.

Наряду с разработкой новых эффективных методов и алгоритмов общим магистральным направлением снижения практических временны́х затрат на решение задач указанного класса остается выбор эффективной модели вычислений на существующих классах архитектур вычислительных систем, что требует соответствующей адаптации методов и алгоритмов к выбранной модели вычислений[3]. В рамках классической модели вычислений А. Тьюринга–Дж. Неймана основным направлением снижения временны́х затрат является распределение требуемого объема информационно-вычислительной работы по совокупности параллельно работающих вычислителей.

Организация параллельных вычислений базируется на совокупности различных подходов. Принципиально важными решениями в повышении производительности параллельных вычислительных систем являются: введение конвейерной организации выполнения команд; включение в систему команд векторных операций, позволяющих одной командой обрабатывать целые массивы данных; распределение вычислений на множество процессоров. Все больше развитие в настоящее время получает и параллельное программирование на графических процессорах современных видеокарт. Наиболее удобный инструмент для организации параллельных вычислений предлагает компания Nvidia.

1. Архитектура CUDA

В статье будем использовать следующие определения и понятия.

Параллельные вычисления (параллельная обработка) – это использование нескольких или многих вычислительных устройств для одновременного выполнения разных частей одной программы.

Задача параллельных вычислений – создание ресурса параллелизма (распараллеливания алгоритмов) в процессах решения задач и управление реализацией этого параллелизма с целью достижения наибольшей эффективности использования многопроцессорной техники.

Параллельный алгоритм – алгоритм, операции которого могут выполняться одновременно[4].

GPGPU – технология использования графического процессора видеокарты для расчетов в приложениях для общих вычислений.

GPU-устройство – видеоадаптер, поддерживающий технологию GPGPU и драйвер CUDA или другое специализированное ус-

тройство, предназначенное для исполнения программ, использующих CUDA (например, Nvidia Tesla).

Host-код – часть программы для архитектуры CUDA, выполняемая на центральном процессоре (CPU).

Kernel-код – часть программы для архитектуры CUDA, выполняемая на GPU- устройстве[5].

Первый комплект инструментов для доступа к инструкциям графического ускорителя был представлен Nvidia в 2007 г.

Nvidia CUDA – это архитектура, т. е. совокупность программных и аппаратных средств, которые позволяют производить на GPU компании Nvidia, поддерживающих технологию GPGPU, вычисления общего назначения.

GPU-устройства имеют свою собственную оперативную память, доступ к которой осуществляется посредством шины PCI-Express. Программа для такой архитектуры состоит из host-кода, написанного на языке C, и kernel-кода, который пишется на специальном языке.

Вычислительная архитектура CUDA основана на концепции «одна команда на множество данных» (*Single Instruction Multiple Data, SIMD*) и понятии мультипроцессора.

При использовании SIMD-устройств надо сформировать последовательность команд, сконфигурировать вычислительные устройства (мультипроцессоры) и передать данные на обработку. Эта последовательность действий для CUDA SDK представлена на рис. 1. Программист пишет kernel-код, который будет обрабатывать множество данных, и задает конфигурацию GPU.

Особенностью архитектуры CUDA является блочно-сеточная организация, необычная для многопоточных приложений. GPU представляет собой массив из отдельных вычислительных ядер.

Использование CUDA предполагает разбиение задачи на независимые части (блоки), которые могут выполняться параллельно. Далее каждый блок разбивается на множество параллельно выполняющихся потоков (thread). CUDA обеспечивает средства расширения языка C для параллельного запуска множества потоков на GPU, выполняющих одну и ту же функцию (ядро). Теоретически максимальный размер ядра – 2 млн инструкций PTX. Потоки объединяются в блоки (до 512 потоков), блоки объединяются в сетки, или решетки (grid). Потоки внутри блока запускаются на одном мультипроцессоре (далее – MP), имеют общую разделяемую память и могут (должны) синхронизовать ход выполнения задачи.

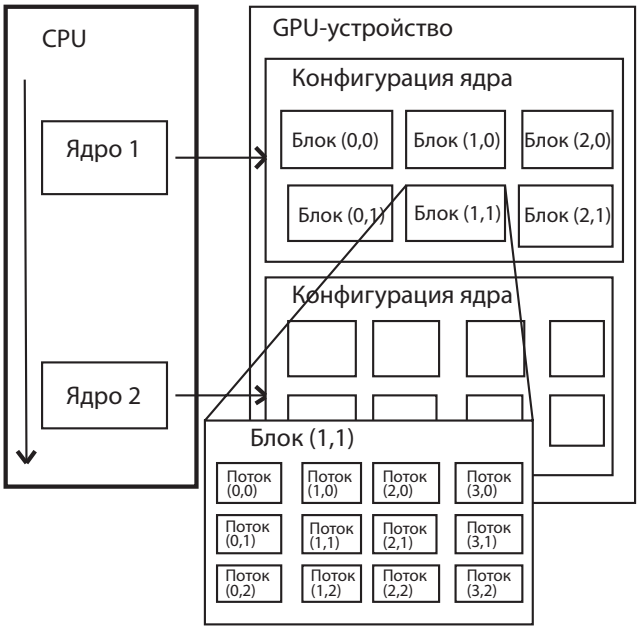


Рис. 1. Элементы конфигурации GPU

MP состоит из «простых» процессоров, пула регистров, разделяемой памяти и планировщика команд. Планировщик команд последовательно разбивает потоки активного блока на порции (warp), по 4 на каждый «простой» процессор и выполняет по одной простой команде одновременно для всех потоков порции за 4 цикла. Для исполнения одной команды порции потоков MP должен загрузить операнды для всех потоков порции, выполнить команду (одновременно), записать результат. По завершению всех потоков блока, ресурсы MP освобождаются, и на него может быть распределен следующий блок.

Количество потоков в блоке и количество блоков в решетке выбирается программистом исходя из максимизации загрузки ресурсов MP и с учетом аппаратных ограничений (количество регистров, разделяемой памяти и т.д.). Блоков должно быть больше числа MP, чтобы не было простоя во время чтения из памяти. Количество потоков в блоке должно быть кратно размеру порции.

При реализации многих алгоритмов на технологической платформе CUDA без их адаптации к архитектуре прироста производительности, как правило, не происходит. Одна из причин этого

в том, что ветвление, выполняемое внутри порции, сильно замедляет работу ядра. Стоит отметить, что не все задачи подходят для SIMD- архитектур. GPU предназначен для вычислений с большим параллелизмом и интенсивной арифметикой. Для эффективного использования графических процессоров нужно стараться разбить алгоритм на такие части, чтобы они могли эффективно выполняться в стиле SIMD. При программной реализации алгоритма необходимо особое внимание уделять выбору и использованию памяти. Например, если все задачи одного блока обращаются к одному и тому же участку памяти или близко расположенным участкам, то следует помещать данные в текстурную или константную память. Для двухмерных данных лучше использовать текстурную память, она специально оптимизирована под двухмерную выборку.

2. Адаптация метода Шермана–Лемана к вычислительной архитектуре CUDA

Для успешной адаптации алгоритма метода Шермана–Лемана[6] надо, во-первых, определить количество вычислительных ядер используемого GPU. Во-вторых, алгоритм метода Шермана–Лемана надо проанализировать на предмет разделения его операций на два класса: выполняемые на CPU и выполняемые на GPU. Выполнять алгоритм целиком на GPU заведомо нецелесообразно, так как без использования CPU не осуществить ввод–вывод данных для обработки GPU, и некоторые операции ветвления быстрее выполнить на CPU. Алгоритм состоит из нескольких этапов[7], поэтому анализ операций и их разбиение на классы придется проводить для каждого этапа.

Алгоритм Шермана–Лемана (модифицированный)

Шаг 1. Проверить делимость числа n на все числа из множества $\{a_i\} = \{3, ..., \lfloor\sqrt[3]{n}\rfloor\}$, все операции этого шага попадают во второй класс и выполняются параллельно для всех чисе a_i. Определим число вычислительных ядер через k. Возможны две ситуации: $h \geq k$ или $h > k$, где $h = |\{a_i\}| = |\{3, ..., \lfloor\sqrt[3]{n}\rfloor\}|$ – количество чисел. Первый случай тривиален, время выполнения первого этапа сократится в k раз. Во втором потребуется организация нескольких шагов, на каждом из которых будет проверяться делимость числа n на очередные k экземпляров a_i. Вообще говоря, количество таких шагов может быть равно $l = \left[\frac{h}{k}\right] + 1$. По окончании каждого шага

необходимо делать вывод о переходе к следующему шагу алгоритма или завершении работы алгоритма. Время реализации первого этапа алгоритма будет равно времени выполнения l операций деления. При последовательном выполнении алгоритма число проверок равнялось количеству операций деления, т. е. $\lfloor \sqrt[3]{n} \rfloor$.

Шаг 2.

2.1. Для всех пар чисел (k, d) $k = 1, 2, \ldots \lfloor \sqrt[3]{n} \rfloor$, $d = 0, 1, \ldots \left\lfloor \sqrt[6]{n} / 4\sqrt{k} \right\rfloor + 1$ проверить выполнение условия

$$d\left(4\sqrt{kn} + d\right) = c^2,\ c \in \mathbf{Z}. \qquad (1)$$

Последнее осуществляется параллельным образом.

2.2. Вычислить величины $A = \lfloor 2\sqrt{kn} \rfloor + d$ и $B = \sqrt{(A^2 - 4kn)}$, соответствующие парам чисел (k, d).

2.3. Для значений A и B, для которых выполнилось условие (1), проверить условие $A^2 \equiv B^2 \pmod{n}$.

Шаг 3. Для значений A и B, прошедших проверку пункта 2.3., проверить выполнение условия $1 < (A \pm B, n) < n$. Если оно выполнено, то делитель найден.

Последнее двойное неравенство целесообразно выполнять на CPU, так как таких проверок мало, а проверка ветвлений на GPU выполняется достаточно медленно.

3. Вычислительный эксперимент

Для экспериментальной оценки эффективности вычислений в архитектуре GPU были задействованы следующие технологические платформы:

– AMD Phenom II (x3) 720 2.80 ГГц, оперативная память 2 Гб;

– Nvidia GeForce GT 240 96 вычислительных ядер CUDA, оперативная память 512 Мб;

– Nvidia GeForce GTX 560 336 вычислительных ядер CUDA, оперативная память 1024 Мб.

Результаты вычислительных экспериментов приведены в таблице.

Как видно, время вычислений при использовании параллельных вычислений на GPU в несколько раз меньше, чем на CPU. Эффективность вычислений зависит от способа распараллеливания алгоритма, при этом время вычислений зависит еще и от технологической платформы GPU.

Как видно из таблицы, при увеличении вычислительных ядер GPU-устройства в 3,5 раза время вычислений сокращается в 2 раза

Таблица

Результаты вычислительных экспериментов

Факторизуемое число ($n = pq$)	Размерность числа (бит)	Время решения t, *ms*		
		CPU, 2,8 Гц, 2048 Мб	GPU, 96 ядер CUDA, 512 Мб	GPU, 336 ядер CUDA, 1024 Мб
223550209643=524287 × 426389	38	9	2,17	0,95
35785968397=2124679 × 16843	36	4	1,9	0,95
17549235333121=16769023 × 1046527	44	11	4,40	2,02

и даже больше. Стоит отметить, что стоимость увеличения производительности в данном случае составляет чуть более 100 долл., что несравнимо со стоимостью любого CPU. При использовании более мощных GPU-устройств или специализированных решений Nvidia следует ожидать прироста производительности в несколько раз и снижения временны́х затрат на несколько порядков.

Выводы

Результаты проведенных вычислительных экспериментов показывают, что адаптация метода Шермана-Лемана к архитектуре CUDA позволяет снизить практические временны́е затраты на решение задачи факторизации целых чисел от нескольких раз до нескольких порядков в зависимости от сомножителей разлагаемого числа. Учитывая, что стоимость простейшей кластерной системы на основе стандартных комплектующих в несколько десятков раз больше, чем стоимость аналогичного по вычислительной мощности GPU-устройства, эффективность и целесообразность использования технологии GPGPU при решении задач факторизации целых чисел очевидна.

Автор выражает глубокую благодарность проф. А.Е. Барановичу за ценные рекомендации и помощь при проведении исследований.

Примечания

[1] См.: *Коблиц Н.* Курс теории чисел и криптографии / Пер. с англ. М.А. Михайловской и В.Е. Тараканова; под ред. А.М. Зубкова. М.: Научное издательство ТВП (Теория вероятностей и ее применения), 2001.

[2] См: *Смарт Н.* Криптография. М.: Техносфера, 2006.

[3] См.: *Баранович А.Е.* Введение в предметно ориентированные анализ, синтез и оптимизацию элементов архитектур потоковых систем обработки данных: Электронное учебно-метод. изд. [Электрон. ресурс] = Introduction in the object-oriented analysis, synthesis and optimization of elements of architecture data flow processing systems. 3-е изд., стереотип., испр. [М.: Информрегистр, 2010].

[4] См.: *Воеводин В.В., Воеводин Вл.В.* Параллельные вычисления. СПб.: БХВ-Петербург, 2002.

[5] См.: *Боресков А.В., Харламов А.А.* Основы работы с технологией CUDA. М.: ДМК Пресс, 2010.

[6] См.: *Баранович А.Е., Желтов С.А.* Организация параллельных вычислений в задачах факторизации на базе архитектуры CUDA // Тр. III Междунар. конгресса по интеллект. системам и информ. технол. / XI Междунар. научн.-техн. конф. «Интеллектуальные системы»(AIS'11). М.: Физматлит, 2011. Т. 1. С. 481–485.

[7] См.: *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.

А.Е. Баранович

СЕМАНТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КРИПТОСЕМАНТИКА

В контексте информационно-эволюционного подхода к системному анализу и моделированию объективной реальности продолжается исследование основных аспектов обеспечения информационной безопасности антропоморфных и антропогенных систем различного генезиса. Основное внимание в настоящей работе сконцентрировано на криптосемантике – новом направлении обеспечения защищенности информационных ресурсов интеллектуальных систем от их несанкционированного использования. Являясь разделом общей криптологии, криптосемантика характеризуется рядом принципиальных отличий от классической криптографии и опирается на собственный аксиоматический базис. Статья продолжает цикл работ, посвященных семантико-прагматическим аспектам обеспечения информационной безопасности.

Ключевые слова: интеллектуальные системы, информационная безопасность, криптология, криптосемантика, семантика.

ВВЕДЕНИЕ

В основе *теоретической криптосемантики* (KS)[1] лежит класс формальных обратимых преобразований семантики засекречиваемой информации (И.), в историческом плане именуемых семантическими шифрами (СШ), в отличие от классических криптографических шифров по К. Шеннону, определяемых на структурно-статистической модели множества открытых сообщений и связанных с преобразованиями их формального семиотико-синтаксического представления в модели Дж. фон Неймана.

Принципиальное отличие KS от криптографии (KG) – использование феноменологии и моделей коммуникационной информации, принципиально отличных от классической интерпретации К. Шеннона, определяемой на априорно заданной структурно-статистической модели множества открытых сообщений (ОС) и связанной с преобразованиями их формального семиотико-синтаксического представления в модели Дж. фон Неймана. В предметной области общей криптологии криптосемантика входит в перечень таких ее существенно феноменологически различимых направлений, как криптография, стеганография и т. п. (см. рис. 1).

Вторичный, порожденный термин «криптосемантика» («тайное значение, скрытый смысл») синтезирован (по аналогии с криптографией) из первичных словоформ древнегреческого языка:

– *κρυπτος* (в совокупности с однокоренными *κρυπτον, κρυπτοω*) – тайна, тайный, потайной, секретный, скрытный и т.п., и,

– *σημαντικος* – обозначающий, обозначение, значение (смысл) и т. п.[2]

Проблемы исследования семантической и аксиологической сторон И. в криптографии, и поиск новых классов шифров, отличных от классических, традиционных, относятся к фундаментально–методологическим исследованиям в области криптологии (KL).

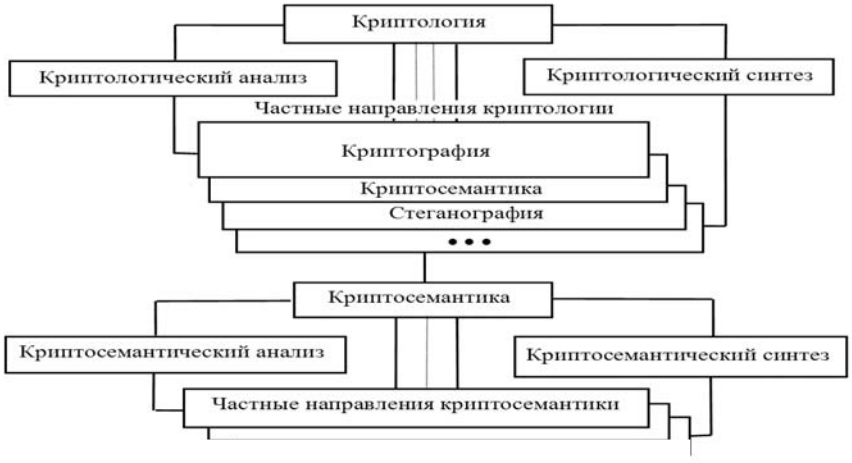


Рис.1. Общая структура криптологии

I. РЕТРОСПЕКТИВА

Понятие СШ неоднократно упоминалось в истории KL, возникнув фактически одновременно с общим содержательным понятием шифра как обратимой процедуры преобразования сообщений во вполне определенном и ограниченном коллективе абонентов социально-коммуникационной среды, скрывающей (искажающей) их содержание[3] от любого индивидуума вне данного коллектива. Практически все теологические источники знаний, от протоарийского комплекса и даосизма до Евангелий и сур Корана, в той или иной форме использовали иносказание, т. е. общеупотребительную лексику и терминологию, в отличном от обыденного сознания смысле. Одни из первых европейских систематизированных трудов по теории и практике шифровального дела Леона Альберти «Трактат о шифрах» (1466) и Иоганнеса Тритемия «Полиграфия» (1499) также содержат ряд примеров практического использования СШ. Особый интерес к KS на рубеже XVII–XVIII вв. возродили члены масонских лож: «По традиции, сложившейся в Европе, в своей переписке масоны использовали особые шифры. Внешне, в своем большинстве они выглядели как шифры простой замены, где буквы алфавита заменялись особыми графемами... Однако, это были гораздо более сложные, так называемые семантические[4] шифры...»[5]

Неформальный обзор криптографических и некриптографических методов и способов засекречивания И. дал Дэвид Кан в своей популярной книге «The Codebreakers»[6]: «Лингвистические стеганограммы подразделяются... на... семаграммы и условное-письмо ... В жаргонном коде внешне безобидное слово имеет совершенно другое реальное значение в тексте, составленном так, что он выглядит как можно более невинно и правдоподобно... До тех пор пока жаргонный код не привлекает к себе внимания, он вполне надежен... Коды составляются на лингвистической основе... в то время как в шифрах этого нет... В решетке Кардана имеющие значение слова располагаются на странице в определенных местах... Разговорный жаргон[7]... примыкает к арго... Арго – специализированный словарь, употребляющийся в различных социальных группах[8]... в него входит... большое число необходимых технических терминов[9]; он служит признаком того, что говорящий принадлежит к ограниченному кругу лиц... Когда говорящие на арго хотят скрыть свои мысли, они могут изменить либо значение слова, либо его форму. Арго в течение сотен лет был секретным

языком... благодаря присущим ему криптографическим свойствам[10]».

Для обозначения предметной области анализа открытой И. (множества «открытых сообщений» по, К. Шеннону) на наличие в ней секретных сведений Д. Кан использует заимствованный термин «энигматология», подчеркивая, что он «дает возможность не употреблять термин “криптография” для некриптографии» и «позволяет не называть “шифром” то, что не является шифром». При этом Д. Кан приводит множество примеров, иллюстрирующих, с его точки зрения, случаи поиска секретных сведений в заведомо незасекреченной И., т. е. случаи бессмысленного криптологического анализа: «...Проблема энигматологии является по своей природе не логической, а психологической... Энигмадукции являются классическими примерами стремления выдать желаемое за действительное... Они представляют собой патологию криптографии».

Здесь мы вынуждены не согласиться с некоторыми формально-логическими выводами Д. Кана, не исключая, естественно, и случай действительной энигмадукции, связанной с иллюзорными воззрениями криптоаналитика:

1. Д. Кан опирается на семиотическую (с вполне определенными синтаксисом и морфологией) модель открытого текста (ОТ), не имея представления, например, о множественной семантической интерпретации одной и той же семиотической структуры, когда одному ОТ σ в семиотической модели при определенных условиях может соответствовать несколько ОТ в семантической модели (фактически несколько различных «смыслов» σ).

2. Процедура засекречивания смысла сообщения может быть смоделирована в модифицированной аксиоматике и терминологии моделей классического криптографического шифра (KG-шифра). Именно поэтому секретные преобразования смысла И. (ее содержания, в отличие от формы в KG) получают у нас впоследствии наименование криптосемантических шифров (KS-шифров), а не неопределенных математически «энигмадукций».

3. Необычен с поверхностной точки зрения, но достоверен факт, что любой открытый текст под произвольной формой несет в себе скрытую семантическую И., особенности проявления которой связаны с характеристиками подсистемы знаний (ПЗ) воспринимающей И. интеллектуальной системы (ИС)[11].

4. СШ могут быть включены в область стеганографии только при условии скрытия факта передачи засекреченной И.[12], что на самом деле не является необходимым условием их использования, хотя и создает дополнительные трудности для KS-анализа.

Замечание Д. Кана о том, что «жаргонные коды или двусмысленные сообщения... основаны на использовании человека в качестве шифровального устройства», базируется на классическом антропном подходе[13] к анализу семантики. Постнеклассический же подход позволяет интерпретировать «антропный» интеллект в качестве одного из возможных уровней организации интеллекта в целом как эволюционного механизма адаптивного метауправления высокоорганизованной системой[14]. В соответствии с вышесказанным, KS-шифры могут быть реализованы универсальными (в том числе антропогенными) «интеллектуальными» устройствами, включающими механизмы прямого и обратного преобразования семантики И.

Что касается учета семантики в классической KG, то Д. Кан (со ссылкой на У. Макфарлейна) пишет: «Криптограф не интересуется содержанием телеграмм: для него имеет значение лишь аналитическое раскрытие шифра». В частности, Дж. Валлис «всегда интересовался не предметом переписки, а лишь чистым искусством криптографии». Таким образом, вопросы семантического анализа до последнего времени не входили в компетенцию специалистов по KG.

В отличие от криптографа, целью криптосемантика является восстановление истинного содержания (исходного смысла первичного сообщения коммуникации) поступающей, возможно засекреченной И. Соответственно, и методология ее достижения существенным образом отличается от методологии решения классических криптографических задач.

Анализ главных требований к шифрам, сформулированных лордом-канцлером Англии, посвященным 33 ступени Великой ложи Розенкрейцеров, Френсисом Бэконом (XVII в.): «Они *не должны поддаваться дешифрованию* (1), *не должны требовать много времени для написания и чтения* (2), и *не должны возбуждать подозрения* (3)», позволяет классифицировать современные криптографические шифры как шифры, практически отвечающие первым двум требованиям и фактически не обеспечивающие выполнение третьего (вне использования методов стеганографии). Одним из важнейших доводов исследования и использования KS-шифров является гипотетическая возможность практического

выполнения для данного класса, наряду с первыми двумя, и последнего требования Ф. Бэкона к «идеальным» шифрам (см. *Утверждение* 2).

Опыт использования эвристического (логико-лингвистического) подхода при анализе KS показал его высокую трудоемкость и концептуальную противоречивость. По результатам исследований, проведенных автором, можно утверждать, что без использования аппарата, основанного на математическом моделировании процессов преобразования семантики И. в системах коммуникации антропоморфных ИС (АИС), провести детальный анализ предметной области KS весьма затруднительно.

II. KS-ШИФРЫ: ПОСЛЕДОВАТЕЛЬНАЯ ЭКСПЛИКАЦИЯ МОДЕЛИ

Модель семантики вербальной коммуникации АИС синтезирована на основе результатов взаимодействия двух математических объектов: семиотической модели Дж. фон Неймана последовательности символов конечного алфавита для представления произвольной семиотической структуры σ и семейства теоретико-графовых экспликаций структуралистической модели-универсума информации[15].

На содержательном уровне экспликации модель семантики произвольной коммуникационной семиотической структуры σ относительно ИС ζ в момент времени f определена как динамически активизированная в процессе «восприятия–осмысления» ($f \geq f_k$, где f_k – конечное значение интервала «восприятие– распознавание» σ) подмодель модели ПЗ ИС $Z^{\sigma}_{\zeta f}$, характеризуемая отображением

$$F : \sigma \times Z_{\zeta f} \rightarrow Z^{\sigma}_{\zeta f}, Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f}, \qquad (1)$$

где $Z_{\zeta f}$ – модель состояния (открытой либо замкнутой) ПЗ ИС ζ в момент времени f и σ представлена моделью последовательности символов конечного алфавита $A \equiv \{a_1,...,a_z\}, |A| = Z$

$$\sigma_i \equiv \sigma_{i_1},...,\sigma_{i_l}, l \le L < \infty, \sigma_{i_j} \in A$$
$$для\ \forall\ i, j,\ j = \overline{1,l},\ i = \overline{1,N}, N \le \sum_{k=1}^{L} z^k \qquad (2)$$

Используем модели (1)– (2) (первичный уровень экспликации содержательного аспекта семантики) в качестве исходного аппарата синтеза основ формальной аксиоматической теории KS.

Объекты σ и $Z^{\sigma}_{\zeta f}$, задействованные в выражении (1), обладают вполне определенным свойством симметрии, что позволяет рассмотреть и следующее отображение

$$F' : Z^{\sigma}_{\zeta f} \times Z_{\zeta f} \to \sigma, Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f} \qquad (3)$$

В условиях стационарности текущего (мгновенного) состояния модели ПЗ $Z_{\zeta f}$, независимости $Z_{\zeta f}$ от конкретной σ и фиксированного вида отображений F, F' выражения (1), (3) представимы в виде

$$\sigma \underset{Z_{\zeta f}}{\overset{F}{\to}} Z^{\sigma}_{\zeta f}, Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f}$$
$$Z^{\sigma}_{\zeta f} \underset{Z_{\zeta f}}{\overset{F'}{\to}} \sigma, Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f} \qquad (4)$$

Выражения (4) фактически определяют некоторые ограниченные подмножества декартовых произведений $\{Z^{\sigma}_{\zeta f}\} \times \{\sigma\}$ и $\{\sigma\} \times \{Z^{\sigma}_{\zeta f}\}$, представленных упорядоченными парами элементов $(Z^{\sigma}_{\zeta f}, \sigma)$ и $(\sigma, Z^{\sigma}_{\zeta f})$.

Из сюръективности отображений (4)[16] следует, что для $\forall Z^{\sigma}_{\zeta f}$, $Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f}$ может быть идентифицирована модель σ как элемент известного множества $\{\sigma\}$ или новый элемент $\tilde{\sigma}$, синтези-

рованный из модели $Z^{\sigma}_{\zeta f}$ путем ее лингвистической редукции, согласно абстракции потенциальной осуществимости[17]. Причем при задании фиксированной схемы кодирования[18] абстрактной экспликации модели[19] множество $\{Z^{\sigma}_{\zeta f}\}$ однозначным образом порождает (см. (4)) мультимножество семантически распознаваемых структур $\{\sigma\}$ (для $\forall Z^{\sigma}_{\zeta f}$ с точностью до *s*-эквивалентности σ[20])[21]. Конечность структуры $Z_{\zeta f}$ при «разумной» схеме кодирования (ограничениях на потенциальную размерность N в выражении (3.2)) определяет конечность множества $\{Z^{\sigma}_{\zeta f}\}$, а соответственно, и конечность множества $\{\sigma\}$, $|\{Z^{\sigma}_{\zeta f}\}| \le |\{\sigma\}|$. Таким образом, для $\forall Z^{\sigma}_{\zeta f}$ существует конечное число допустимых пар $(Z^{\sigma}_{\zeta f}, \sigma)$.

В то же время условие конечности ПЗ ИС (априорное условие АИС) предопределяет возможность синтеза структур σ', для которых не существует образа $Z^{\sigma'}_{\zeta f}$, $Z^{\sigma'}_{\zeta f} \subseteq Z_{\zeta f}$. Образ $Z^{\sigma'}_{\zeta f}$ не формируется и для случаев нераспознавания σ (формы ее представления в классической KG). Фактически имеет место множественное отображение $\{\sigma'\} \underset{Z_{\zeta f}}{\overset{F}{\rightarrow}} \varnothing$[22]. Таким образом, пары $(\sigma, Z^{\sigma}_{\zeta f})$ определены на ограниченном подмножестве потенциально существующих $\{\sigma\}$.

В результате может быть определено конечное число неупорядоченных пар $(Z^{\sigma}_{\zeta f}, \sigma) \equiv (\sigma, Z^{\sigma}_{\zeta f})$, тождественных с точностью до *s*-эквивалентности. Иллюстрация соотношений (3.4) представлена

на рис. 2, где $Z^{\sigma}_{\zeta f} \subseteq Z_{\zeta f}$, $\sigma_1,...,\sigma_k \in \{\sigma\}$, $k \geq 0$, $\sigma^{\zeta}_{r} \underset{s}{\overset{f}{\sim}} \sigma^{\zeta}_{t}$ $\forall r,t = \overline{1,\kappa},$[23] $\{\sigma'\} \bigcap \{\sigma\} \equiv \varnothing, |\{\sigma'\}| \neq 0$, $\tilde{\sigma} \notin \{\sigma\}$ – допустимая синтезированная семиотическая структура ($k = 0$).

Изменение семантики $Z^{\sigma}_{\zeta f}$ при организации секретной коммуникации в среде АИС с целью скрытия ее первичного значения («смысла» исходной И.) от возможных нежелательных участников коммуникации («противника») может быть реализовано следующими криптологическими преобразованиями.

1. Изменение (преобразование) структуры σ, моделирующей универсальный групповой коммуникативный код (в частности, текстуальную форму естественного языка коммуникации). Фактически речь здесь идет о секретном преобразовании формы представления И. В вышеупомянутых работах[24] показано, что в общем случае изменения σ порождают и изменение семантики $Z^{\sigma}_{\zeta f}$. Исследованием различных видов секретных преобразований σ как формы представления И. (KG-шифры, коды) без явного использования ее семантических характеристик занимается классическая (теоретическая) KG. При этом семантический анализ существующих криптографических систем показывает, что используемые в них преобразования σ обеспечивают и решение задачи секретного изменения семантики сообщений.

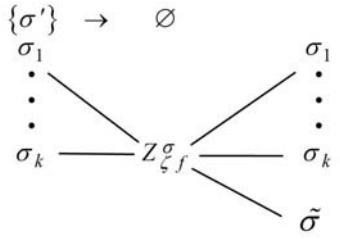


Рис.2. Структура элементов модели семантики

Согласно методологии данного пункта, реализация совершенного в некотором смысле KG-шифра может быть сведена к выбору преобразования $f:\sigma\to\hat{\sigma}$, обеспечивающего $Z^{\hat{\sigma}}_{\zeta f}\equiv\varnothing$ в коллективной модели знаний предметной области коммуникации[25], для любых АИС ζ за исключением некоторого конечного подмножества абонентов системы секретной коммуникации (ССК) $\{\xi\}\subset\{\zeta\}$. Здесь σ – исходная семиотическая структура (открытое сообщение), $Z^{\sigma}_{\zeta f}\not\equiv\varnothing$, а $\hat{\sigma}$ – результирующая структура, преобразованная методами KG (шифрованное сообщение). В частности, представление преобразованной $\hat{\sigma}$ в виде случайной равновероятной последовательности символов конечного алфавита произвольной длины порождает совершенно «бессмысленное», по известным, вполне определенным критериям[26], сообщение, когда идентифицировать семантику $Z^{\hat{\sigma}}_{\zeta f}$ не представляется возможным.

Знание обратного преобразования $f^{-1}:\hat{\sigma}\to\sigma$ позволяет на основе соотношения (3.1) восстановить исходную семантику $Z^{\sigma}_{\zeta f}$.

2. Изменение $Z^{\sigma}_{\zeta f}$ без изменения структуры σ. Из соотношения (3.1) следует, что данное преобразование можно реализовать только путем изменения непосредственно $Z_{\zeta f}$. При этом учитываются условия, налагаемые на универсальность отображения F[27], когда компонента отображений в системе семантической коммуникации представима универсальным выражением для всех участников коммуникации, в то время как индивидуальная компонента отображения F_{ζ} АИС ζ полностью характеризуется состоянием индивидуальной ПЗ $Z_{\zeta f}$.

Именно данный класс преобразований $Z^{\sigma}_{\zeta f}$ связан с представлением и индивидуальной интерпретацией И. (фактически с

семантикой И.) в ПЗ произвольных ИС, т. е. непосредственным образом входит в предметную область KS.

3. Изменение $Z^{\sigma}_{\zeta f}$ в соответствии с преобразованиями п. 1–2, а именно путем изменения и σ и $Z_{\zeta f}$. Очевидно, что данный класс преобразований сводится к двум предыдущим и, с учетом стеганографических свойств KS-шифра (скрытие факта засекречивания при неизменности σ), принадлежит области KL. Вследствие априорной ограниченности объема настоящей работы основное внимание в ней уделено исследованию класса преобразований п. 2.

III. KS-ШИФРЫ: ОСНОВЫ АКСИОМАТИЧЕСКОЙ ТЕОРИИ

Пусть задана фиксированная семиотическая структура σ (открытый текст в KG), имеющая для заданной АИС ζ в состоянии f семантику $Z^{\sigma}_{\zeta f}$, и для системы семантической (s-)коммуникации определено выполнение условий s-стационарности и s-($s\varepsilon$-)эквивалентности[28]. Пусть также определены фиксированные конечные множества X, K и Y, соответственно, открытых текстов (в криптографическом смысле), ключей и секретных (шифрованных) текстов.

Определение 1. Криптосемантический шифр (KS-шифр) в широком смысле $\mathcal{A}_a$ есть обратимое преобразование И., связанное с изменением ее семантики, моделируемое четверкой математических объектов

$$\mathcal{A}_a : < Z_a, K_a, W_a, f_a > \qquad (5)$$

где Z_a, K_a, W_a – конечные множества, соответственно, моделей открытых семантик И., ключей и моделей засекреченных семантик И. (для фиксированных KS-шифров положим $\mathcal{A} : < Z, K, W >$).

Сюръективное отображение f_a (функция KS– шифрования)

$$f_a : Z_a \times K_a \to W_a \qquad (6)$$

инъективно при любом фиксированном ключе $\kappa \in K_a$. Другими словами, частичные функции $f_{a_k} : Z_a \to W_a$ инъективны при всех $\kappa \in K_a$.

Уравнения KS– шифрования / расшифрования имеют общий вид

$$f_a(z,k) \equiv w, f_a^{-1}(w,k) \equiv z, \ z \in Z, w \in W, k \in K, \qquad (7)$$

причем в силу инъективности функции f_a, $|Z| \le |W|$ и $f_a^{-1}(w,k)$ определены для всех $w \in f_a^{-1}(Z,k)$ ◁

Нетрудно видеть, что в формулировке (5)– (7) KG-шифр есть частный случай KS-шифра, когда в условиях использования каналов передачи с ограниченной пропускной способностью модель семантики представляется в виде последовательной семиотической модели Дж. фон Неймана (2).

Введенное определение в явном виде не содержит указателей на реально используемые формы (универсальные коды) *s*-ком– муникации АИС. Модифицируем его, конкретизируя особенности возможной реализации KS-шифра. Прежде всего это касается определения множества коммуникационных форм представления И. В частности, непрерывные аналоговые преобразования речи, оптические преобразования И. в криптоиедографии[29] или квантовой KG[30] (для непрерывной модели преобразований) не вкладываются в известную криптографическую дискретную модель текста. Учитывая обилие возможных коммуникационных форм представления семантики и ориентируясь на конечную физическую пропускную способность каналов коммуникации, остановимся на вербальных средствах коммуникации, т. е. представлении коммуникационных форм множеством вполне определенных кодовых семиотических структур $\{\sigma\}$.

Определим в качестве множества коммуникационных семиотических структур $\{\sigma\}$ в модели KS-шифра множество *открытых сообщений* X по К. Шеннону, представленное семейством структурно-статистических моделей Дж. фон Неймана различного

уровня приближения к естественному языку (ЕЯ) в его «обыденной» интерпретации[31]. Предложения ЕЯ, полученные *иконическими* методами, вполне удовлетворяют характеристическим свойствам вышеупомянутых моделей.

Определение 2. Криптосемантический шифр в узком смысле $\mathcal{A}_a$ есть обратимое преобразование И., связанное с изменением ее семантики, моделируемое пятеркой математических объектов

$$\mathcal{A}_a : < Z_a, K_a, W_a, X_a, f_a >, \tag{8}$$

($\mathcal{A} : < Z, K, W, X >$ для случая фиксированного KS-шифра), где Z_a, K_a, W_a, X_a – конечные множества, соответственно, моделей открытых семантик И., ключей, моделей секретных семантик И. и семиотических коммуникационных структур $\{\sigma\}$, представленных ОС ЕЯ классической KG, $f_a \equiv \{f_a^1, f_a^2\}$.

Сюръективные отображения f_a^1 (функция KS-шифрования) и f_a^2

$$\begin{aligned} f_a^1 &: Z_a \times K_a \to W_a \\ f_a^2 &: W_a \to X_a \end{aligned} \tag{9}$$

инъективны при любом фиксированном ключе $\kappa \in K_a$ (частичные функции $f_a^1 : Z_a \times K_a \to W_a$, $f_a^2 : W_a \to X_a$ инъективны при всех $\kappa \in K_a$).

Уравнения KS-шифрования / расшифрования имеют общий вид

$$\begin{aligned} & f_a^1 (Z_{\zeta f}^{\sigma}, \kappa) \equiv Z_{\zeta f}^{\hat{\sigma}}, \; f_a^2 (Z_{\zeta f}^{\hat{\sigma}}) \equiv \hat{\sigma} \\ & f_a^{2^{-1}} (\hat{\sigma}) \equiv Z_{\zeta f}^{\hat{\sigma}}, \; f_a^{1^{-1}} (Z_{\zeta f}^{\hat{\sigma}}, \kappa) \equiv Z_{\zeta f}^{\sigma} \\ & Z_{\zeta f}^{\sigma} \in z, \; Z_{\zeta f}^{\hat{\sigma}} \in W, \hat{\sigma} \in X, \kappa \in K \end{aligned} \tag{10}$$

или в сокращенном виде (при введении обозначений $f_a^* \equiv (f_a^1, f_a^2)$, $f_a^{*-1} \equiv (f_a^{2^{-1}}, f_a^{1^{-1}})$ – как суперпозиции операций; порядок следования определен)

$$f_a^*(Z_{\zeta f}^{\sigma}, k) \equiv \hat{\sigma},$$
$$f_a^{*-1}(\hat{\sigma}, k) \equiv Z_{\zeta f}^{\sigma}, \qquad (10')$$
$$Z_{\zeta f}^{\sigma} \in z, \ \hat{\sigma} \in X, \ k \in K,$$

причем в силу инъективности функции f_a^*, $|Z| \le |X|$, и $f_a^{*-1}(\hat{\sigma}, \kappa)$ определены для всех $\hat{\sigma} \in f_a^*(Z, \kappa)$ $\triangleleft$

При сокращенной форме записи KS-шифра возможно использование формализма $\mathcal{A}: <Z, K, Y>, Y \equiv X$, где Y – множество засекреченных сообщений, представленных элементами $\hat{\sigma} \in X$ (*автоморфный* KS-шифр[32]).

Введение модели KS-шифра позволяет с нестандартных позиций взглянуть на основные объекты, используемые в классической KG. Действительно, что есть множества «открытых» и «секретных» («шифрованных») сообщений (СС) в KG и KS? Относительно KG представители указанных множеств различаются по вполне определенным вероятностно-алгебраическим критериям, характеризующим меру их «близости» по своим статистико-структурным свойствам к представителям иконического множества ЕЯ. Однако существуют и контрфакты, противоречащие данной процедуре. Например, использование «качественной» γ (KG-гаммы) в качестве представителя множества ОС с KG-преобразованием ее перед передачей по каналу связи. Более того, та же γ, переданная по каналу связи при отсутствии KG-преобразования (ошибка в ССК), не содержит признаков принадлежности ее к множеству ОС. В результате в KS необходимым образом формируется собственная аксиоматико-терминологическая система основных понятий предметной области.

В отношении автоморфных KS-шифров справедливы следующие утверждения.

Утверждение 1. Необходимым и достаточным условием однозначной идентификации в аксиоматической системе классической KG элементов множеств «открытых» и «секретных» сообщений в *автоморфных* KS-системах является *непосредственный указатель* источника (инициатора) коммуникации (в ситуации его безусловной семантической истинности[33]) ◁

Доказательство. Произвольные представители семиотической модели фон Неймана в автоморфных KS-шифрах порождают тождественные множества «открытых» и «секретных» сообщений. В отличие от множеств «открытых» и «шифрованных» (секретных) сообщений в классической криптографии (модели коммуникации по К. Шеннону[34]), единственным отличительным признаком элементов множеств ОС и СС в KS, в общей постановке, является непосредственный указатель (признак) источника ОС Из чего следует: а) необходимость: если указатель отсутствует, задача определения принадлежности сообщения к множествам ОС или СС, в общей постановке классической KG-неразрешима; б) достаточность: если указатель присутствует, в условиях безусловной семантической истинности И. (в указателе) ОС однозначно различимо с СС ◁◁

Утверждение 2. В условиях семантической стационарности ($st\lambda$-) системы коммуникации[35] для автоморфного KS-шифра выполняется *третье условие совершенности шифра* по Ф. Бэкону[36] ◁

Доказательство. Вследствие выполнения условия стационарности использования KS-шифра (стационарность автоморфизма $Y \to Y$) при отсутствии непосредственного указателя источника коммуникации на секретность И. СС *неотличимо* от ОС и «не должно *возбуждать подозрения*» при контроле системы коммуникации сторонними лицами, что обеспечивает выполнение третьего условия совершенности шифра по Ф.Бэкону. ◁◁

Утверждение 3. Для любого сообщения σ в автоморфном KS-шифре выполняется соотношение $Z^{\sigma}_{\zeta f} \not\equiv \varnothing$ (наличие «гипотетического» смысла). ◁

Доказательство. По определению автоморфного KS-шифра. ◁◁

Утверждение 4. Во вполне определенных условиях задания случайного автоморфизма на корпусе «открытых» сообщений $Y \equiv X$ длины l в модели Дж. фон Неймана соответствующий автоморфный KS–-шифр есть $l-$ совершенный шифр по К. Шеннону ◁

Доказательство. Необходимое и достаточное условие для *совершенности шифра по К. Шеннону*[37] есть выполнение условия $P(x/y) = P(x)$ для всех $x \in X$ и $y \in Y$, т. е. *условия независимости* $P(y/x)$ *от* x, где X и Y – множества, соответственно, открытых и секретных сообщений, $P(x/y) = P(x)\,P(y/x)/P(y)$ (по теореме Байеса), $P(x)$ – априорная вероятность ОС x, $P(y/x)$ – условная вероятность СС y при условии, что выбрано ОС x, $P(y)$ – вероятность СС y и $P(x/y)$ – апостериорная вероятность ОС x при условии, что перехвачено СС y.

Схема случайного автоморфизма $X \to X$ в процедуре синтеза СС y в автоморфном KS-шифре эквивалентна классической урновой схеме *случайного выбора сообщения* x из X мощности $|X|$, определяемого в качестве СС y. При организации процедуры *случайного равновероятного* выбора СС из множества ОС его выбор никоим образом не связан с конкретным ОС x, что в полной мере отвечает выполнению *условия независимости* $P(y/x)$ *от* x.

Условие же l-совершенности есть *ослабленное условие* совершенности К. Шеннона для случая множества X, сформированного сообщениями σ из (2) фиксированной длины l, что в совокупности с вышесказанным обеспечивает выполнение данного условия для автоморфного KS-шифра. ◁◁

Условие l-совершенной стойкости в KS, как и в KG, обеспечивает независимость выбора СС y от ОС x, но сохраняет при этом длину сообщения x, известную третьей стороне. Мощность допустимого множества ключей (симметричной группы подстановок) при этом есть функция от l, ограниченная значением сверху $(z^l)!$, где z – мощность алфавита ЕЯ. В отношении модели фон Неймана (2) известен целый ряд оценок мощности множеств допустимых представителей ЕЯ, полученных как иконическими методами, так и методами конструктивного модельного синтеза (различной степени приближения к ЕЯ на длинах до $l = 25$)[38].

Следствие 1 *к Утверждению* 4. В условиях задания случайного автоморфизма утверждения 4 на полном корпусе «открытых» сообще-

ний $Y \equiv X$ в модели Дж. фон Неймана, соответствующий автоморфный KS-шифр есть *совершенный шифр по К. Шеннону* $\triangleleft$

Доказательство. При отказе от фиксированной длины l сообщения x и переходе к понятию совершенности (обобщенной) шифра по К. Шеннону условия следствия выполняются вследствие сохранения схемы случайного выбора сообщения x на полном множестве X (сообщений σ сколь угодно большой длины), определяемого в качестве СС y, что в полной мере сохраняет и условия независимости $P(y/x)$ от x $\triangleleft\triangleleft$

Следует заметить, что для KS-шифра дополнительные условия совершенности, как, например, неограниченность ключа[39], в общем случае не существенны вследствие, как уже отмечалось, принципиальных различий KS- и KG-шифров[40]. В автоморфных KS-шифрах множества ОС и СС не различимы с использованием KG-критериев, что влечет использование вышеупомянутых KS-указателей или KS-критериев различения искомых множеств. При отсутствии критериев идентификации KS-шифров наблюдатель не имеет возможности выделить KS-сообщения из информационного потока и, либо вынужден идентифицировать их как истинные, либо отбраковывать весь информационный поток при условии возможного KS-шифрования.

К числу возможных подходов к синтезу методов идентификации иконических KS-сообщений в потоке открытой информации можно отнести подход, основанный на семантическом анализе сцепленного потока сеансовых сообщений в наблюдаемой ССК $\hat{\sigma}_1 \circ \hat{\sigma}_2 \circ \hat{\sigma}_3 \circ \ldots$ (контекстный анализ) и выявлении в нем семантических противоречий, т. е. противоречий в объединенной семантике $Z_{\zeta f}^{\hat{\sigma}_1 \circ \hat{\sigma}_2 \circ \hat{\sigma}_3 \circ \ldots}$ по отношению к ПЗ $Z_{\zeta f}$ наблюдающей системы ζ. Для искусственно синтезируемых в ИС текстов ЕЯ множества СС семантический анализ возможен и для случая выделенных сеансовых $\hat{\sigma}$ вследствие задействования в любой конечной антропогенной ИС лингвистических моделей ограниченного уровня приближения к ЕЯ. Универсальнообщим методом выявления случаев использования KS-шифров является практическая проверка «оперативных ситуаций», характеризуемых содержанием (семантикой) сообщений.

ЗАКЛЮЧЕНИЕ

Содержательную основу различия теоретических KS и KG составляют различия в используемых моделях представления и использования И. об объективной реальности, когда KG-модели опираются на принцип независимости модели сообщений от характеристических индивидуальных свойств абонентов системы секретной коммуникации, в то время как модели KS-сообщений принципиальным образом связаны с моделированием субъективных (семантико-прагматических) характеристик ИС. Дальнейшему изложению основ криптосемантики, включая понятие обобщенного криптологического (KL-) шифра и вопросы синтеза практической процедур реализации процессов KS- и KL-шифрования планируется посвятить последующие работы цикла.

Примечания

[1] См.: *Баранович А.Е.* Семантические аспекты информационной безопасности: концентрация знаний // Вестник РГГУ. 2011. № 13 (75).Сер. «Информатика. Защита информации. Математика». С. 38—58.
См.: *Баранович А.Е.* Некоторые семантико-прагматические механизмы информационной безопасности / Системы высокой доступности. 2011. № 2. С. 84—89

[2] См.: *Дворецкий И.Х.* Древнегреческо-русский словарь. Под ред. чл.-кор. АН СССР С.И. Соболевского: В 2 т. Т. 1 (А—Л). М.: Гос. изд-во иностр. и научн. словарей, 1958.

[3] Классическая KG в качестве основного инструмента скрытия содержания (смысла) сообщений выбрала методы и способы изменения формы его представления, что в определенных условиях влечет и изменение его смысла в отношении к абонентам среды коммуникации.

[4] Точнее, члены «Братства франкмасонов» использовали на практике комбинированный криптологический шифр (KL-шифр), в основе которого лежал СШ, усложненный криптографическим шифром простой замены.

[5] См. *Бабаш А.В., Шанкин Г.П.* История криптографии. М.: Гелиос АРВ, 2002.
См.: *Бабаш А.В., Шанкин Г.П.* Криптография. М.: Солон-пресс, 2007.; см.: Масонство в его прошлом и настоящем / Под ред. С.П. Мельгунова и Н.П. Сидорова: В 2 т. Репринтное изд. 1914. М.: МКПА, 1991.

[6] См.: *Kahn D.* The Codebreakers. N.Y.: The Macmillan Company, 1967.

[7] См. также «сленг» (от англ. *slang*).

[8] Примером русифицированного арго является блатной жаргон «феня».

[9] См.: *Быков В.* Русская феня. Словарь современного интержаргона асоциальных элементов. Смоленск: ТРАСТ-ИМАКОМ, 1993.

[10] На примере арго как усовершенствования жаргонного кода мы отмечаем использование методов KG (изменение формы), и методов KS (изменение значения).

[11] См.: *Баранович А.Е.* Универсальный подход к структурному моделированию директивно-целевых информационных процессов. Автоматная модель интеллектуального процесса оценки ценности информации на Х-гиперграфах: Сб. статей. М.: ГШ ВС РФ, 1997. С. 2–22.
См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах. М.: ГШ ВС РФ, 2002.

[12] См.: Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: Солон-Пресс, 2002 (Сер. «Аспекты защиты»).

[13] См.: *Казютинский В.В.* Антропный принцип в неклассической и постнеклассической науке // Проблемы методологии постнеклассической науки: Сб. ст. / Отв. ред. Е.А. Мамчур; РАН. Ин-т философии. М.: ИФРАН, 1992.
См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу. М.: РГГУ, 2011.

[14] *Баранович А.Е.* О систематизации аксиоматического аппарата предметной области «Искусственный интеллект» / Интеллектуальные системы. 2010. Т. 14. Вып. 1–4. С. 5–34; см.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения.

[15] См.: *Баранович А.Е.* Универсальный подход к структурному моделированию директивно-целевых информационных процессов.
См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах.
См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: ГШ ВС РФ, 2003.

[16] См.: *Баранович А.Е.* Универсальный подход к структурному моделированию директивно-целевых информационных процессов.
См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах.

[17] См.: Математический энциклопедический словарь. Гл. ред. Ю.В. Прохоров. М.: Сов. энциклоп., 1988.

[18] См.: *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[19] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.

[20] Семантической эквивалентности коммуникации

[21] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах

[22] Для случая $Z^{\sigma}_{\zeta f} \equiv \varnothing$ семантика σ относительно МС ζ в состоянии f не определена.

[23] *s*-эквивалентность в момент (интервал) времени f.

[24] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах
См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения.

[25] В частности, вне сферы KL, в которой $Z^{\hat{\sigma}}_{\zeta f} \not\equiv \varnothing$ для любых сообщений.

[26] См.: *Бабаш А.В., Шанкин Г.П.* Криптография.

[27] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах.

[28] Стационарные условия *s*-коммуникации (*s*-стационарность), *s*-эквивалентность и s-стационарность

[29] См.: *Kahn D.* Op. cit.

[30] См.: Advances in cryptology // Proceedings EUROCRYPT'90. 1990.

[31] Переход от классической модели множества текстов по Дж. фон Нейману–К. Шеннону к другим формам представления семантики требует незначительных усилий по формальной модификации получаемых результатов.

[32] Условие $|Y|=|X|$ в теории KG-шифров используется при определе-нии *эндоморфного* шифра, причем KG-шифр $\mathcal{A}$ является эндоморфным *в узком смысле*, если $X \equiv Y$. Однако, несмотря на формальное сходство, KS-шифры принципиально отличимы от KG-шифров. В эндоморфном KG-шифре (как, впрочем, и в любом другом KG-шифре) речь идет о преобразовании форм представления И. (на шенноновской модели ОТ), когда ее семантические аспекты не принимаются во внимание. Сущность же KS-шифрования заключается в преобразованиях семантики. При этом выбор семиотической структуры $\hat{\sigma} \in X$ как коммуникативной формы представления И есть частный случай реализации вербальной коммуникации КС. В общем же случае KS-шифрования форма представления коммуникационной И. может быть произвольной (например, артикуляционной или образной). Согласно опр. 3.2, необходимо лишь обеспечить принадлежность используемых форм представления И. (семантики) в коммуникационной среде известным, т. е. открытым и общедоступным коммуникативным формам, связанным естественным изоморфизмом с общепринятой семантикой И.

[33] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах

[34] См.: *Shannon C.E., Weaver W.A.* The Mathematical Theory of Communication. Urbana: University of Illinois Press, 1949 (Пер. в кн.: *Шеннон К.* Работы по теории информации и кибернетике. М.: Иностр. лит-ра, 1963. С. 243–322)

[35] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах.

[36] См. *Бабаш А.В., Шанкин Г.П.* История криптографии.
См.: *Kahn D.* Op. Cit.

[37] См.: *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Изд-во иностранной литературы, 1963. 830 с.

[38] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.
См.: *Иглицкая С.М.* К вопросу структурно-алгебраического и семантико-прагматического анализа музыкального текста // Вестник РГГУ. 2011. № 13(75). Сер. «Информатика. Защита информации. Математика». С. 128–145.

[39] См.: *Зубов А.Ю.* Совершенные шифры: вступ. сл. чл.-кор. РАН Б.А. Севастьянова. М.: Гелиос АРВ, 2003.

[40] Автоморфный KS-шифр в исходной постановке не относится к классу *потоковых* (KG-) шифров.

А.С. Зайцев, А.А. Малюк

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ВНУТРЕННЕГО НАРУШИТЕЛЯ

В статье подробно рассматривается проблема внутреннего нарушителя. Производится комплексный анализ проблемы, рассматриваются существующие модели инсайдера. На основе произведенного анализа строится имитационная системно-динамическая модель внутреннего нарушителя, позволяющая дать финансовые оценки. Далее производится попытка формализации модели с использованием экспертного опроса. Рассматриваются варианты дальнейшего развития модели для минимизации участия эксперта в оценке.

Ключевые слова: инсайдер, системная динамика, имитационное моделирование, экспертная система.

Проблема внутреннего нарушителя (инсайдера) является одним из наиболее актуальных вопросов современной информационной безопасности (ИБ). Судить о ситуации с инсайдерами, однако, возможно лишь по немногочисленным аналитическим отчетам. Наиболее актуальным и полным из них, на наш взгляд, является аналитическое исследование компании Perimetrix «Инсайдерские угрозы в России 2009»[1], составленное согласно анонимному опросу представителей российских компаний. На рис. 1 приведены самые популярные внутренние угрозы (по мнению респондентов Perimetrix).

Согласно другому аналитическому исследованию, выполненному компанией InfoWatch («Глобальное исследование утечек. Первое полугодие 2010»[2]), самой критической категорией информации стали персональные данные (97,9% утечек).

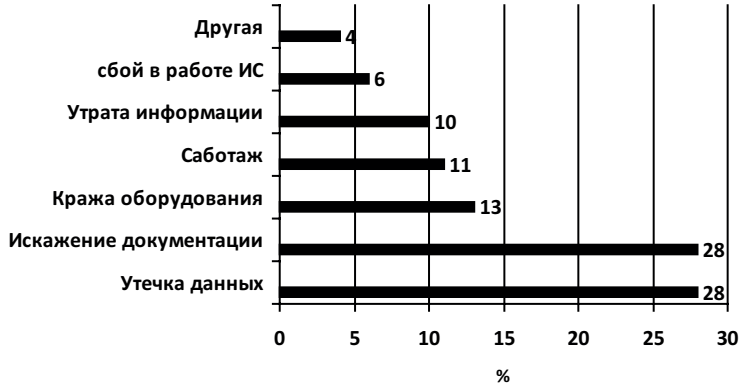


Рис. 1. Самые популярные внутренние угрозы информационной безопасности

В некоторых странах, например в США, предприятия обязаны передавать в соответствующие органы информацию о произошедших инцидентах в области нарушения компьютерной безопасности. Но значит ли это, что компания передаст соответствующую действительности картину внутренних нарушений? Согласно аналитическому исследованию, проведенному Carnegie Mellon University («2011 CyberSecurityWatch Survey»[3]), 76% опрошенных компаний не разглашают сведений о произошедших внутренних инцидентах ИБ (рис. 2).

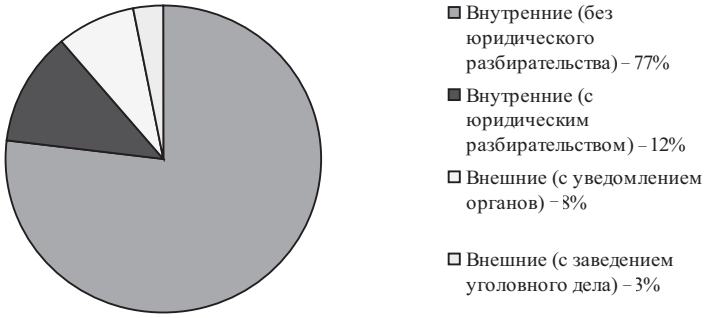


Рис. 2. Меры, применяемые по отношению к инсайдеру согласно статистике Carnegie Mellon University

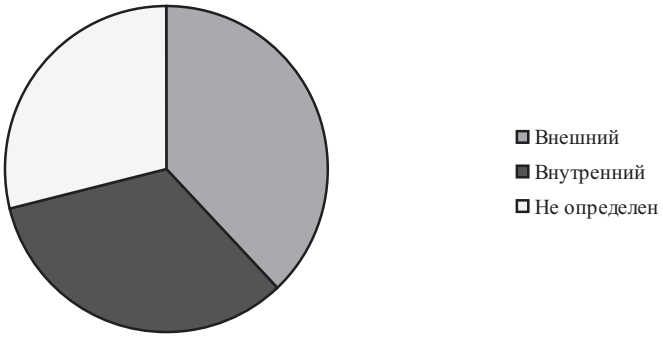


Рис. 3. Убытки от различных типов инцидентов по отношению к общим потерям ИБ согласно статистике Carnegie Mellon University

Причем по состоянию на первый квартал 2011 г., инциденты с инсайдерами составляют 21% относительно всего числа инцидентов ИБ (инциденты с аутсайдерами – 58%, в 21% случаев источник не определен).

Согласно этому же отчету, инциденты, связанные с внутренними нарушителями, приносят компаниям бóльшие убытки, чем аутсайдерские инциденты ИБ (рис. 3).

На сегодняшний день существует ряд объективных причин, препятствующих эффективному решению проблемы внутреннего нарушителя. Среди них наибольшее значение имеют:

– отсутствие достаточной статистики внутренних инцидентов;

– отсутствие методологии управления внутренними инцидентами (формализованные модели нарушителей, системы оценки рисков, методы управления рисками и инцидентами);

– сильнейшее влияние человеческого фактора (действия нарушителя сложно моделировать и прогнозировать);

– репутационные риски, сложно поддающиеся оценке и формализации;

– непонимание важности проблемы руководством компаний.

Ключевым моментом в решении практически всех этих проблем является построение модели внутреннего нарушителя.

На данный момент известны несколько моделей внутреннего нарушителя[4]. Все они фактически представляют собой неформальные классификации по одному или нескольким критериям. Рассмотрим некоторые из них.

Таблица 1

Классификация инсайдеров в зависимости от мотивации

Немотивированный (нарушитель, который сознательно не хотел причинить ущерб компании)	Халатный:	Как правило, это инцидент случайного нарушения прав доступа, случайного удаления информации. Наиболее часто встречается вынос информации за пределы компании для работы дома	
	Манипулируемый	Как следствие распространения методов социальной инженерии, манипулируемый инсайдер встречается довольно часто. Сотрудник может отправить конфиденциальную информацию злоумышленнику исходя из лучших побуждений и даже не понимая, что его действия могут нанести вред	
Мотивированный (в данном случае имеется пара «внутренний–внешний злоумышленники». Внутренний нарушитель вследствие каких-либо причин действует так, как ему говорит находящийся вне компании человек)	Обиженный	Такой сотрудник стремится нанести вред компании по личным мотивам. Особенность такого нарушителя заключается в том, что он стремится передать (уничтожить) информацию, опираясь на собственные представления о ценности данной информации	
	Мотивированный	Подрабатывающий	Такой нарушитель работает на внешнего злоумышленника вследствие каких-то причин (деньги, шантаж, угрозы), но не хочет в дальнейшем покидать компанию
		Специально внедренный	Такой нарушитель может обладать техническими средствами. При этом он будет всеми силами стараться совершить необходимое ему действие, чего бы это ни стоило

Таблица 1 представляет модель, наиболее полно отражающую возможные мотивации поступков внутренних нарушителей.

В зависимости от уровня полномочий сотрудника внутренние нарушители могут быть разделены на четыре группы, показанные в табл. 2.

Таблица 2

Классификация инсайдеров в зависимости от их полномочий

Уровень	Полномочия
1	Самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации
2	Возможность создания и запуска собственных программ с новыми функциями по обработке информации
3	Возможность управления функционированием АС, т. е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования
4	Весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации

Таблица 3

Классификация инсайдеров в зависимости от их должности

Уровень риска	Пользователь
Наибольший риск	Сетевой администратор Администратор безопасности
Повышенный риск	Оператор системы Оператор ввода и подготовки данных Менеджер обработки Системный программист
Средний риск	Инженер системы Менеджер программного обеспечения
Ограниченный риск	Прикладной программист Инженер или оператор по связи Администратор баз данных Инженер по оборудованию Оператор периферийного оборудования Библиотекарь системных магнитных носителей Пользователь-программист Пользователь-операционист
Низкий риск	Инженер по периферийному оборудованию Библиотекарь магнитных носителей пользователей Пользователь сети

Известно еще множество вариаций такого подхода к классификации, но ничего существенного они не добавляют. К примеру, классификация по полномочиям участников корпоративной сети приведена в табл. 3.

Таким образом, изначальным критерием классификации внутреннего нарушителя является его мотивация. Опираясь на мотивацию нарушителя, попытаемся сформулировать подходы к формализации его модели. Чтобы модель не получилась слишком громоздкой, распределим нарушителей по следующим группам: немотивированные, обиженные, нелояльные, специально внедренные.

Будем считать, что немотивированные включают в себя халатных и манипулируемых, а специально внедренные объединяют тех, кто собирается уволиться после совершения нарушения, и тех, кто желает продолжить работу в организации. На количество внутренних нарушителей каждого типа влияют различные факторы (табл. 4).

Таблица 4

Факторы, влияющие на инсайдеров различных типов

Тип инсайдера	Влияющие факторы
1	2
Немотивированный нарушитель	Осведомленность сотрудников о системе обеспечения ИБ (о хранении паролей и др.) Наличие системы защиты данных на рабочих станциях (шифрование и др.) Установлена ли ответственность за нарушение ИБ Установлена ли ответственность за работу вне офиса Ведется ли резервное копирование данных Производится ли классификация данных и установление различных уровней доступа к ней Установлена ли контентная фильтрация трафика Насколько эффективно ведется подготовка новых специалистов Ведется ли контроль съемных устройств
Обиженный нарушитель	Понимает ли он ответственность на нарушение ИБ Реально ли оценивает нарушитель важность информации Степень и причины обиды: недостаточная оценка деятельности низкая зарплата низкая должность личная обида другие причины

1	2
	Моральное состояние коллектива Поведение человека до нарушения Наличие уголовной ответственности (эффективность работы кадровой службы) Установлена ли контентная фильтрация трафика Ведется ли контроль съемных устройств
Нелояльный нарушитель	Понимает ли нарушитель ответственность за нарушение ИБ Подписаны ли документы о неразглашении конфиденциальной информации Имеет ли нарушитель доступ к актуальной информации (работа кадровой службы) Наличие системы защиты данных на рабочих станциях (шифрование и др.) Установлена ли ответственность за нарушение ИБ Ведется ли резервное копирование данных Производится ли классификация данных и установление различных уровней доступа к ним Установлена ли контентная фильтрация трафика Ведется ли контроль съемных устройств
Специально внедренный нарушитель	Установлена ли в документах ответственность за нарушение ИБ Наличие системы защиты данных на рабочих станциях (шифрование и др.) Установлена ли контентная фильтрация трафика Ведется ли контроль съемных устройств Установлена ли система регистрации действий сотрудников (с другой стороны, такая система может ухудшать атмосферу в коллективе) Материальное и психологическое состояние нарушителя Атмосфера в коллективе Степень мотивированности нарушителя на получение информации Работа мониторинга психологического состояния сотрудников Наличие предыстории сотрудника (работа кадровой службы)
Все типы внутренних нарушителей	Текучесть кадров на предприятии Подготовка новых кадров (испытательный срок, наличие опытного куратора, семинары и психологическое тестирование)

Стоит отметить, что одним из ключевых моментов противодействия инсайдерам является эффективность работы кадровой службы.

Разделим все факторы, влияющие на нарушителей, на две группы: *априорные факторы*, влияющие на предотвращение появления самого инцидента нарушения, и *апостериорные факторы*, позволяющие провести разбор произошедшего инцидента нарушения.

Одним из основополагающих *априорных факторов* несомненно является работа кадровой службы. Рассмотрим в связи с этим более подробно процесс набора и увольнения персонала. Основным здесь является текучесть кадров, т. е. движение рабочей силы, обусловленное неудовлетворенностью работника рабочим местом или неудовлетворенностью организации конкретным работником[5]. Численно текучесть может быть определена как отношение числа уволившихся работников в год к общему числу работников. Текучесть бывает естественной (3–5% в год) и излишней. Излишняя текучесть плохо влияет на атмосферу в коллективе. В свою очередь, плохая атмосфера в коллективе вызывает излишнюю текучесть.

На текучесть и, следовательно, на атмосферу в коллективе влияют, на наш взгляд, три основных фактора: уровень зарплат, различные поощрения, наличие социального пакета и прочие условия труда; качество работы кадровой службы; различные меры и мероприятия, направленные на сплочение коллектива, например корпоративные мероприятия.

Отмеченные в описании типов нарушителей факторы сгруппируем в пять основных групп: обучение сотрудников методам обеспечения информационной безопасности; уведомление сотрудников об ответственности за нарушение информационной безопасности (данный фактор можно использовать более эффективно, если в документах действительно зафиксирована конкретная ответственность); организационные меры защиты (к ним отнесем классификацию данных, разграничение доступа и работу службы охраны); атмосфера в коллективе; технические меры защиты (шифрование на рабочих станциях, резервное копирование информации, контентную фильтрацию исходящего трафика, системы контроля съемных устройств).

Апостериорные факторы заключаются в разборе произошедшего инцидента и применении или неприменении установленных санкций. Причем инцидент может быть разобран только в случае,

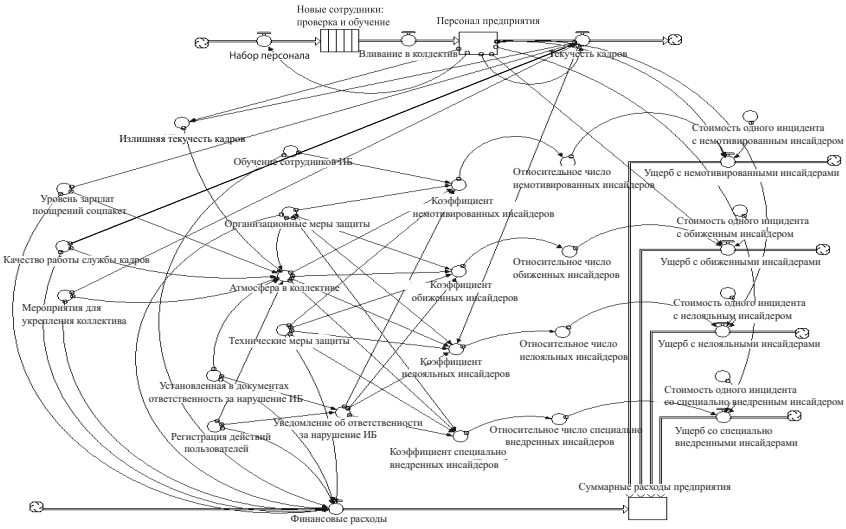


Рис. 4. Системно-динамическая модель внутреннего нарушителя

если ведется регистрация действий пользователей (для сбора доказательной базы) и все документы имеют юридическую силу с установлением ответственности за нарушение информационной безопасности.

Модель должна предусматривать применение мер к виновнику происшествия. В результате это усилит значимость дальнейших уведомлений об ответственности за нарушение информационной безопасности, но в то же время может негативно сказаться на атмосфере в коллективе.

Эффективность моделируемой системы обеспечения безопасности может определяться минимизацией суммы средств, потраченных на предотвращение инцидентов, и потерь, связанных с произошедшими нарушениями.

В качестве методологической основы моделирования представляется целесообразным использовать системную динамику Форрестера, которая позволяет строить формальные модели сложных систем[6]. Установив связи между описанными выше факторами, получим при помощи пакета имитационного моделирования iThink системно-динамическую диаграмму, представленную на рис. 4.

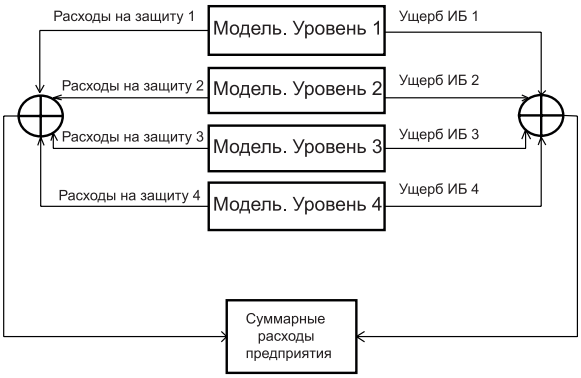


Рис. 5. Объединение моделей различных групп пользователей

Данная модель не учитывает, однако, реально существующего различия уровней пользователей в зависимости от полномочий и, соответственно, различной ценности информации, к которой они имеют доступ. Поэтому (подобно принципу достаточной глубины контроля доступа в защите от НСД) для некоторой информации и пользователей просто нецелесообразно применять высокие меры защиты, а для более высоких уровней необходимо применение усиленной защиты.

Этот недостаток можно компенсировать, используя модель, предложенную в руководящем документе Гостехкомиссии[7]. Для этого введем четыре категории пользователей и информации, к которой они имеют доступ, и применим модель отдельно к каждой из этих категорий. Финансовые расходы будем получать в виде суммы расходов каждой категории. Данные действия иллюстрируются на рис. 5.

Для удобства дальнейшего использования и реализации углубленного анализа все элементы модели были разбиты по группам, все существенные элементы были описаны и им даны условные обозначения (табл. 5).

Большинство из приведенных выше элементов трудно формализуемо. Для получения их значений целесообразно использовать метод анализа иерархий Т. Саати[8]. Данный метод позволяет получить формальные оценки, используя экспертный опрос.

С его помощью можно установить значения следующих элементов: коэффициент немотивированных инсайдеров; коэффи-

Таблица 5

Классификация элементов системы

Название	Описание	Обозначение
1	2	3
Качественные коэффициенты – качественно определяют риски проявления нарушителей того или иного типа.		
Коэффициент немотивированных инсайдеров	0 – 10.0 – нарушителей такого типа нет вообще 10 – число нарушителей такого типа максимально	КЧ_НЕМО
Коэффициент обиженных инсайдеров	0 – 10.0 – нарушителей такого типа нет вообще 10 – число нарушителей такого типа максимально	КЧ_ОБИЖ
Коэффициент нелояльных инсайдеров	0 – 10.0 – нарушителей такого типа нет вообще 10 – число нарушителей такого типа максимально	КЧ_НЕЛО
Коэффициент специально внедренных инсайдеров	0 – 10.0 – нарушителей такого типа нет вообще 10 – число нарушителей такого типа максимально	КЧ_СПЕЦ
Количественные коэффициенты – количественно определяют риски проявления нарушителей того или иного типа		
Относительное число немотивированных инсайдеров	Отношение числа проявившихся немотивированных инсайдеров в год к общему числу сотрудников предприятия	КЛ_НЕМО
Относительное число обиженных инсайдеров	Отношение числа проявившихся обиженных инсайдеров в год к общему числу сотрудников предприятия	КЛ_ОБИЖ
Относительное число нелояльных инсайдеров	Отношение числа проявившихся нелояльных инсайдеров в год к общему числу сотрудников предприятия	КЛ_НЕЛО
Относительное число специально внедренных инсайдеров	Отношение числа проявившихся специально внедренных инсайдеров в год к общему числу сотрудников предприятия	КЛ_СПЕЦ

1	2	3
Управляющие элементы 1-го уровня – элементы, которые можно менять непосредственно для управления коэффициенстами, характеризующими нарушителей		
Обучение сотрудников ИБ	Целое число от 0 до 10. Характеризует эффективность обучения сотрудников предприятия основам информационной безопасности. Имеет финансовый эквивалент	У1_ОБУЧ
Организационные меры защиты	Целое число от 0 до 10. Характеризует эффективность организационных мер защиты, реализуемых на предприятии. Имеет финансовый эквивалент	У1_ОРГМ
Технические меры защиты	Целое число от 0 до 10. Характеризует эффективность технических мер защиты, реализуемых на предприятии. Имеет финансовый эквивалент	У1_ТЕХМ
Управляющие элементы 2-го уровня – элементы, которые можно менять непосредственно, но они влияют на коэффициенты, характеризующие нарушителей, косвенно, путем изменения некоторых других элементов системы		
Уровень зарплат, поощрений, условия труда и социальный пакет	Условия труда. Элемент, который важен для характеристики атмосферы в коллективе и показателя текучести кадров. Целое число от 0 до 10. Характеризует условия труда на предприятии.	У2_УСЛТ
Качество работы службы кадров	Элемент, важный для изменения характеристики в коллективе и показателя текучести кадров. Целое число от 0 до 10	У2_СКАД
Мероприятия для укрепления коллектива	Элемент, важный для характеристики атмосферы в коллективе и показателя текучести кадров. Целое число от 0 до 10	У2_УКРК
Установленная в документах ответственность за нарушение ИБ	Юридические меры. Элемент, являющийся апостериорной мерой для обеспечения ИБ. Целое число от 0 до 10. Влияетна УО_УВЕД и ПСО_АТМК	У2_ЮРИМ
Регистрация действий пользователей	Апостериорная мера для обеспечения ИБ. Целое число от 0 до 10. Влияет на УО_УВЕД и ПСО_АТМК	У2_РЕГД

1	2	3
Управляющий элемент особый – данный элемент, с одной стороны, можно изменять, он влияет на коэффициенты, характеризующие нарушителей, но, с другой стороны, на него самого влияют другие элементы системы		
Уведомление об ответственности за нарушение ИБ	Особый элемент. Зависит от У2_ЮРИМ и У2_РЕГД	УО_УВЕД
Прочие сложно определяемые элементы		
Атмосфера в коллективе	Фактор, сильно влияющий на коэффициенты, характеризующие нарушителей. На него невозможно влиять напрямую, возможно только косвенно, с использованием других элементов. Некоторые элементы в схеме введены только для воздействия на данный элемент системы	ПСО_АТМК
Текучесть кадров	Элемент, похожий на ПСО_АТМК	ПСО_ТЕКК
Прочие статистические элементы		
Ущерб от одного инцидента с немотивированным инсайдером	Статистическое значение	ПСТ_НЕМО
Ущерб от одного инцидента с обиженным инсайдером	Статистическое значение	ПСТ_ОБИЖ
Ущерб от одного инцидента с нелояльным инсайдером	Статистическое значение	ПСТ_НЕЛО
Ущерб от одного инцидента со специально внедренным инсайдером	Статистическое значение	ПСТ_СПЕЦ
Прочие легко определяемые элементы		
Набор персонала	Необходимое число сотрудников предприятия – число сотрудников предприятия	ПЛО_НАБП
Излишняя текучесть кадров	ПСО_ТЕКК – нормальное значение текучести кадров (2% в год)	ПЛО_ИЗТК

1	2	3
Ущерб с немотивированными инсайдерами	Ущерб ИБ, связанный с инцидентами по вине немотивированных инсайдеров	ПЛО_НЕМО
Ущерб с обиженными инсайдерами	Ущерб ИБ, связанный с инцидентами по вине обиженных инсайдеров	ПЛО_ОБИЖ
Ущерб с нелояльными инсайдерами	Ущерб ИБ, связанный с инцидентами по вине нелояльных инсайдеров	ПЛО_НЕЛО
Ущерб со специально внедренными инсайдерами	Ущерб ИБ, связанный с инцидентами по вине специально внедренных инсайдеров	ПЛО_СПЕЦ
Финансовые расходы	Сумма затрат на все меры по обеспечению ИБ	ПЛО_ФИНР
Персонал предприятия	ПЛО_ПЕРС = ПЛО_ПЕРС + вливание в коллектив – ПСО_ТЕКК	ПЛО_ПЕРС

циент обиженных инсайдеров; коэффициент нелояльных инсайдеров; коэффициент специально внедренных инсайдеров; атмосфера в коллективе; текучесть кадров; уведомление об ответственности за нарушение ИБ (с некоторыми оговорками, см. далее).

Рассмотрим для примера формирование коэффициента немотивированных инсайдеров КЧ_НЕМО. В качестве факторов, влияющих на данный коэффициент, будем рассматривать: обучение ИБ (У_ОБУЧ); уведомление об ответственности (У_УВЕД); организационные меры защиты (У_ОРГМ); атмосфера в коллективе (П_АТМК); технические меры защиты (У_ТЕХМ).

Произведем сравнение выбранных факторов с использованием метода парных сравнений. Оформим результаты экспертизы в виде таблицы (табл. 6), используя шкалу относительного превосходства следующего вида: 1 – равноценность; 3 – умеренное превосходство; 5 – сильное превосходство; 7 – очень сильное превосходство; 9 – высшее (крайнее) превосходство.

Результат сравнения при этом записывается в виде дроби A/1, если фактор по горизонтали, по мнению эксперта, важнее фактора по вертикали в A раз, или 1/B, если фактор по вертикали важнее фактора по горизонтали в B раз. В соответствии с принятой шкалой, числа A и B могут принимать целые значения от 1 до 9. Таблица 6 иллюстрирует эту процедуру для коэффициента немотивированных инсайдеров.

Далее представим все элементы данной таблицы в виде десятичных дробей, суммируем значения элементов по строкам и нормируем сумму. В итоге получим результаты, приведенные в табл. 7.

Таблица 6

Метод парных сравнений (данные эксперта)

Факторы	У_ОБУЧ	У_УВЕД	У_ОРГМ	П_АТМК	У_ТЕХМ
У_ОБУЧ	1/1	1/1	1/2	1/5	1/3
У_УВЕД	1/1	1/1	1/5	1/1	5/1
У_ОРГМ	2/1	1/3	1/1	1/2	2/1
П_АТМК	5/1	1/1	2/1	1/1	1/1
У_ТЕХМ	3/1	1/5	1/2	1/1	1/1

Таблица 7

Нормированные суммы по строкам

Факторы	У_ОБУЧ	У_УВЕД	У_ОРГМ	П_АТМК	У_ТЕХМ	Сумма	Нормиров. сумма
У_ОБУЧ	1	1	0,5	0,2	0,33	3,03	0,092
У_УВЕД	1	1	0,2	1	5	8,2	0,250
У_ОРГМ	2	0,33	1	0,5	2	5,83	0,178
П_АТМК	5	1	2	1	1	10	0,305
У_ТЕХМ	3	0,2	0,5	1	1	5,7	0,174
					Сумма:	32,76	1

Полученные таким образом нормированные значения определяют важность фактора для определения коэффициента немотивированных инсайдеров, который в окончательном виде записывается формулой:

$$КЧ\_НЕМО = 1/5*(0{,}092*(1-У\_ОБУЧ)+$$
$$+0{,}250*(1-У\_УВЕД)+0{,}178*(1-У\_ОРГМ)+$$
$$+0{,}305*(1-П\_АТМК)+0{,}174*(1-У\_ТЕХМ)$$

Данный метод, конечно же, не может считаться точным, однако он позволяет получать значения элементов системы формализованным путем при отсутствии статистического материала.

Если в предлагаемом опросе принимает участие не один эксперт, а целая группа экспертов, то возникает необходимость некоторым образом определять правдоподобность и адекватность оценок каждого нового эксперта. Целесообразно для этого воспользоваться аппаратом математической статистики. Тогда среднее значение каждого коэффициента, полученное с помощью экспертного опроса, может быть выражено формулой:

$$\bar{a} = \frac{1}{n} \sum_{i=l}^{n} a_i.$$

Среднеквадратичное отклонение этой величины будет равно:

$$s = \sqrt{\frac{1}{n} \sum_{i=l}^{n} (a_i - \bar{a})^2}.$$

После накопления достаточного числа экспертной информации для дальнейшего повышения уровня адекватности оценок можно воспользоваться процедурой фильтрации экспертных оценок. По правилу трех сигм (трех s), если отклонение любого коэффициента, получаемого из оценки эксперта, превышает 3*s, то с вероятностью 99,7% оценка такого эксперта оказывается неадекватной, и данные, введенные этим экспертом, необходимо отбраковать, а самого эксперта исключить из дальнейших опросов, считая его недостаточно компетентным.

Далее встает вопрос перевода коэффициента нарушителей в относительное число таких нарушителей по сравнению со всей численностью сотрудников предприятия в год (для которого определяется число инцидентов). Если умножить относительное число нарушителей какого-либо типа в год на среднюю стоимость одного такого инцидента, то можно получить также величину ущерба, наносимого предприятию за счет инцидентов данного типа.

Для перевода коэффициента некоторого типа нарушителей в относительное число нарушителей данного типа необходимо использование доступной статистики.

Допустим, что мы обладаем статистикой инцидентов на конкретном предприятии. Тогда можно определить значения относительного числа нарушителей определенного типа в год по сравнению со всей численностью сотрудников (число данных инцидентов/общее число сотрудников предприятия). Для этого разобьем

полученные выше значения на 10 последовательных групп с равным количеством точек. Далее возьмем среднее значение в группе 1 и получим значение относительного числа нарушителей для коэффициента нарушителей, равного 1. Например, для немотивированных нарушителей будем иметь:

$$\text{КЛ\_НЕМО(КЧ\_НЕМО)} = \begin{cases} \frac{10}{n} * \sum_{i=\frac{n}{10}*(\text{КЧ\_НЕМО}-1)}^{i=\frac{n}{10}*\text{КЧ\_НЕМО}} a(i), \text{ при \_КЧ\_НЕМО} > 0 \\ 0, \text{ при \_КЧ\_НЕМО} = 0 \end{cases}$$

Ущерб от реализации одного инцидента определенного вида может быть определен, исходя из имеющейся статистической информации. При наличии таких данных можно определить ущерб от реализации угроз определенного типа, например для случая с немотивированными инсайдерами, следующим образом:

ПЛО_НЕМО = КЛ_НЕМО (КЧ_НЕМО)*
ПСТ_НЕМО*ПЛО_ПЕРС

Таким образом, мы получаем количественный финансовый показатель для каждого типа инсайдерских угроз.

Далее для реализации нашей модели необходимо определить следующие элементы системы: уровень зарплат, поощрений, социальный пакет; качество работы службы кадров; мероприятия для укрепления коллектива; обучение сотрудников ИБ; организационные меры защиты; регистрацию действий пользователей; технические меры защиты; установленную в документах ответственность за нарушение ИБ.

Каждый из перечисленных элементов представляет собой совокупность одного из чисел от 0 до 10 и денежного эквивалента, т. е. суммы, которую необходимо потратить, чтобы достичь данного уровня управляющего элемента.

Задать эти характеристики можно, оценивая уже существующие системы и выработав с помощью экспертов рекомендации о внедрении необходимых изменений для достижения требуемых значений управляющего элемента, либо путем проведения экспертизы определить набор требований для каждого из уровней управляющего элемента. Первый из указанных способов не обладает достаточной универсальностью и малоприменим на практике.

Если говорить о втором способе, то, например, для достижения уровня 7 элемента «Технические меры защиты», необходимо применять следующий комплекс мер: контекстную фильтрацию по уровню 7; средства для контроля портов по уровню 7; шифрование жестких дисков рабочих станций по уровню 7. Для достижения уровня 10 необходимо применять систему защиты Data Loss Protection уровня 10.

Удобнее всего это реализовать в виде некоторого экспертного центра, в котором все средства защиты будут проходить сертификацию и им будет присваиваться соответствующий уровень. Здесь будут также формироваться пакеты требований для достижения определенного уровня. Финансовый показатель при этом будет определяться как средний из всех возможных пакетов требований данного уровня. Аналогичным образом определяются все остальные управляющие элементы. Остается единственный неопределенный элемент схемы «Уведомление об ответственности за нарушение ИБ». Для моделирования его необходимо задавать вручную, имея в виду, что он в то же время зависит от элементов «Установленная в документах ответственность за нарушение ИБ» и «Регистрация действий пользователей».

Процедура его определения может выглядеть следующим образом. Априорно уведомление об ответственности за нарушение ИБ не может быть действенным без апостериорных методов, которые позволяют установить факт нарушения ИБ и наказать его виновника. Таким образом, элемент «Уведомление об ответственности за нарушение ИБ» не может быть больше значения некоторой совокупности действенности апостериорных методов.

Определим вспомогательный коэффициент возможного максимального значения «Уведомления об ответственности за нарушение ИБ», используя метод парных сравнений для анализа иерархий Т. Саати. Само значение «Уведомления об ответственности за нарушение ИБ» администратор системы может при этом задавать от 0 до некоторого максимального значения.

Все приведенные методы так или иначе используют экспертный опрос. В то же время для уменьшения влияния субъективности и повышения точности моделирования желательно минимизировать участие экспертов. Рассмотрим возможность использования для этого нейронной сети, позволяющей смоделировать действия человека, имитируя его поведение[9].

Нейронная сеть позволяет в применении к нашему случаю заменить неизвестную функцию зависимости выходной переменной от входных (рис. 6).

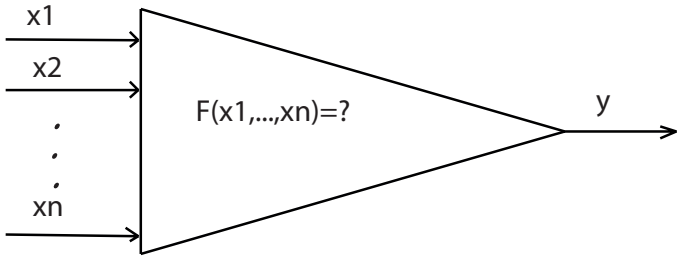


Рис. 6. Нейронная сеть с одной выходной переменной

Нейроны обучаются на имеющейся статистике наборов входных и выходных параметров, и в дальнейшем нейронная сеть способна установить зависимость выходного параметра от входных (смоделировать неизвестную функцию F) при неизвестных в процессе обучения входных параметрах.

Применительно к данной работе на нейронных сетях можно моделировать функционирование таких элементов, как «Коэффициент немотивированных инсайдеров» и «Относительное число немотивированных инсайдеров», «Коэффициент обиженных инсайдеров» и «Относительное число обиженных инсайдеров», «Коэффициент нелояльных инсайдеров» и «Относительное число нелояльных инсайдеров», «Коэффициент специально внедренных инсайдеров» и «Относительно число специально внедренных инсайдеров», «Атмосфера в коллективе», «Текучесть кадров», «Уведомление об ответственности за нарушение ИБ».

Коэффициенты нарушителей были приведены в паре с их количественными характеристиками ввиду того, что нейронная сеть позволит напрямую связать меры защиты с относительным числом немотивированных инсайдеров, минуя дополнительные элементы. Это также положительно скажется на точности системы (так как уменьшение количества последовательно идущих трудноформализуемых элементов уменьшает погрешности, связанные с формализацией).

Но реализовать всю систему в виде одной большой нейронной сети невозможно, так как в этом случае в силу вступает так называемое проклятие размерности нейронных сетей: количество статистического материала, необходимого для обучения нейронной

сети растет нелинейно при возрастании числа входных переменных. Тем самым нет возможности обеспечить статистическим материалом «большую» нейронную сеть.

В нашем случае целесообразно создать нескольких мелких легкообучаемых нейронных сетей, объединяемых в систему при помощи методов имитационного моделирования (рис. 7).

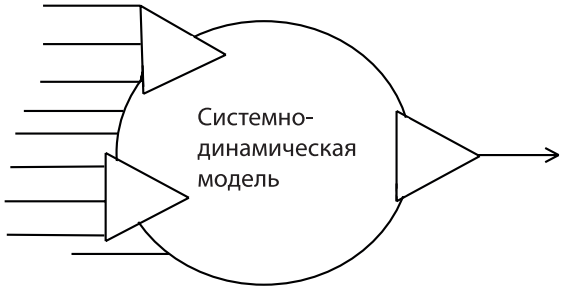


Рис. 7. Построение системы в виде нескольких нейронных сетей, объединенных при помощи имитационного моделирования

При использовании методологии, приведенной в данной статье, будут решены такие проблемы, как проблема формализации человеческого фактора в системе и проблема нехватки статистического материала для построения аналитических и управленческих систем в области информационной безопасности.

Примечания

[1] См.: Инсайдерские угрозы в России 2009 [Электронный ресурс] // Сайт Perimetrix. [М., 2009]. URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf (дата обращения: 06.01.2012).

[2] См.: Глобальное исследование утечек конфиденциальной информации. Первое полугодие 2010 [Электронный ресурс] // Сайт Infowatch. [М., 2010]. URL: http://www.infowatch.ru/sites/default/files/report/infowatch_global_data_leakage_report_2010_russian.pdf (дата обращения: 01.07.2010).

[3] См.: 2011 CyberSecurityWatch Survey [Электронный ресурс] // Сайт Carnegie Mellon University. [М., 2011]. URL: http://www.cert.org/archive/pdf/ CyberSecuritySurvey2011Data.pdf (дата обращения: 06.01.2012).

[4] См.: Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. Концепция защиты средств

вычислительной техники и автоматизированных систем от несанкционированного доступа к информации; ГОСТ 17799-05: Практические правила управления информационной безопасностью. [Электронный ресурс] [М., 2005]. URL: http://docs.cntd.ru/document/1200044724 (дата обращения: 06.01.2012); *Биячуев Т.А.* Безопасность корпоративных сетей. СПб., 2004.

[5] См.: Текучесть кадров [Электронный ресурс] // Сайт ГК «Баланс». [М., 2011]. URL: http://www.balans.ru/ru/library/8/article_39.html (Дата обращения: 06.01.2012).

[6] См.: *Форестер Дж.* Индустриальная динамика. Основы кибернетики предприятия. М.: Прогресс, 1961; *Сендж П.* Пятая дисциплина. Искусство и практика самообучающейся организации. М.: Олимп-Бизнес, 2006.

[7] См.: Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

[8] См.: *Саати Т.* Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993.

[9] См.: *Рассел С., Норвиг П.* Искусственный интеллект. Современный подход. М.: Вильямс, 2007.

В.Р. Григорьев, А.П. Никитин

ИСПОЛЬЗОВАНИЕ СТАТИЧЕСКИХ МЕТОДОВ ДЛЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Рассматривается задача аутентификации пользователя персонального компьютера по его клавиатурному почерку. Предложен подход, позволяющий реализовать систему идентификации пользователя персонального компьютера по особенностям его работы с клавиатурой. Для решения задачи идентификации пользователей предложено использовать статистические методы. Показано, что среди рассмотренных методов наибольшая эффективность для идентификации пользователя достигается путем использования критерия Манна–Уитни.

Ключевые слова: клавиатурный почерк, идентификация пользователя, биометрическая идентификация.

Клавиатурный почерк относится к динамическим (поведенческим) биометрическим характеристикам, описывающим подсознательные действия, привычные для пользователя. Его информативность давно уже стала предметом исследований с точки зрения его использования в задачах идентификации и аутентификации пользователей[1].

Задача аутентификации пользователя персонального компьютера возникла практически тогда же, когда появились сами персональные компьютеры. Изначально основным методом решения данной задачи служили пароли или же разнообразные электронные ключи.

Однако минусы данных подходов состоят в том, что их стойкость гарантируется в основном техническими методами и сильно страдает от так называемого человеческого фактора. Ключ может

быть утерян или украден, а пароль, особенно сложный, забыт или использован другим лицом. Все это может с легкостью привести к компрометации сколь угодно надежной системы безопасности.

В настоящее время доказано, что применение биометрических способов аутентификации пользователя позволяет с высокой эффективностью решать проблемы, присущие традиционным методам аутентификации. В задачах аутентификации пользователя клавиатурный почерк характеризует динамику ввода парольной фразы с помощью клавиатуры. Стандартная клавиатура позволяет измерить следующие временные характеристики: время удержания клавиши нажатой и интервал времени между нажатиями клавиш.

Клавиатурный почерк могут характеризовать и другие параметры, описанные в работе[2]: общее время набора парольной фразы, частота возникновения ошибок при наборе, факт использования дополнительных клавиш (использование числовой клавиатуры), особенности ввода заглавных букв (использование клавиши Shift или Caps Lock) и т. д.

Использование клавиатурного почерка не требует установки специальных аппаратных средств и кадров для установки и поддержки, является прозрачным для конечного пользователя, т. е. не причиняет неудобств пользователю и позволяет проводить скрытую аутентификацию. Клавиатурный почерк также позволяет проводить реаутентификацию для подтверждения личности пользователя перед выполнением критичных операций. Кроме того, клавиатурный почерк обладает всеми преимуществами, присущими биометрическим методам аутентификации[3].

Так как для аутентификации пользователя используются такие параметры, которые не могут быть переданы другому лицу, забыты или потеряны, то это позволяет сильно снизить влияние человеческого фактора на систему безопасности и тем самым повысить предсказуемость ее поведения и надежность. Также в силу высокой индивидуальности этих данных (например, вероятность того, что у двух людей будут одинаковые отпечатки пальцев, составляет $2{,}4*10^{-7}$) возможно построение на их основе систем идентификации пользователей, что представляется совершенно невозможным при использовании традиционных методов.

Таким образом, разработка новых методов биометрической идентификации пользователя сохраняет актуальность и на сегодняшний день.

Далее в данной работе будет предложен метод применения статистических критериев для идентификации пользователя посредством использования динамических биометрических параметров (клавиатурного почерка).

Идентификация личности по клавиатурному почерку

Одной из достаточно сложных задач, повседневно решаемых многими людьми, является быстрый ввод текстов с клавиатуры компьютера. Обычно быстрого клавиатурного ввода информации удается достичь за счет использования всех пальцев обоих рук, при этом у каждого человека появляется свой уникальный клавиатурный почерк. Следует подчеркнуть, что уникальный личный почерк вырабатывается и при ежедневном решении более простой задачи передачи информации кодом Морзе, что использовалось ранее для идентификации личности телеграфиста по его почерку.

Современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью, что позволяет с достаточной вероятностью идентифицировать пользователя, работающего с клавиатурой. Применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре. В противном случае вероятность неправильного опознания легального пользователя существенно возрастает и делает непригодным данный способ идентификации на практике. Исходя из теории машинописи и делопроизводства, можно определить время становления почерка – работы с клавиатурой, при котором достигается необходимая вероятность идентификации пользователя, примерно 6 месяцев.

Данный метод идентификации пользователя представляет наибольший интерес с точки зрения практического применения в связи со следующими его особенностями по сравнению с другими перечисленными методами:

- отсутствие необходимости в дополнительном оборудовании;
- возможность динамического контроля психофизического состояния оператора ЭВМ;
- незаметность и прозрачность метода сбора данных.

Задача биометрической идентификации

Основное отличие задачи аутентификации от задачи идентификации состоит в том, что не пользователь должен доказывать свою личность, а система – распознавать пользователя. Наиболее серьезные различия между данными задачами проявляются тогда, когда ставится задача незаметной для пользователя идентификации. Требование незаметности процедуры идентификации накладывает серьезные ограничения на выбор методов решения данной задачи. Например, становится невозможным использование любых методов, требующих от пользователя каких-либо специфических действий, прямо указывающих на проведение процедуры идентификации.

Необходимость незаметности задачи идентификации может быть обусловлена следующими причинами: 1) проверка легитимности пользователя, зарегистрированного ранее каким-либо другим способом; 2) проведение мероприятий, направленных на борьбу с противоправными действиями отдельных граждан.

Еще более усложняет задачу требование незаметной идентификации пользователя удаленного персонального компьютера. Очевидно, что невозможно гарантировать на удаленном компьютере наличие какой-либо специализированной аппаратуры, предназначенной для проведения процедуры идентификации. Несмотря на широкое распространение встроенных в компьютер и внешних по отношению к нему веб-камер, строить универсальную систему идентификации на их основе в настоящее время нельзя, потому что данное устройство не является обязательным для каждого персонального компьютера. Таким образом, единственно возможными остаются динамические способы идентификации, основанные на использовании стандартных устройств компьютера – клавиатуры и мыши.

Задача незаметной идентификации пользователя удаленного персонального компьютера имеет ряд особенностей, влияющих на выбор конкретного метода ее решения, по сравнению с задачей аутентификации, успешно решаемой в последнее время:

– различное оборудование компьютеров, на которых может работать пользователь;

– использование для идентификации различных текстов и сравнение их с контрольным;

– вероятность того, что текст, применяемый для идентификации, не будет являться осмысленным.

Подводя итог всему вышесказанному, можно утверждать, что идентификация пользователя по его клавиатурному почерку представляет собой практически единственный на сегодняшний день способ решения задачи незаметной идентификации пользователя персонального компьютера.

Алгоритм идентификации пользователя

Для проведения процедуры идентификации пользователя необходимо создать формализованный образ его действий – некий набор параметров, позволяющих однозначно определить пользователя. В данной работе предлагается использовать следующий набор параметров:

- время удержания каждой клавиши;
- время между нажатием на первую и на последнюю клавиши сочетания из n клавиш;
- время между нажатием первой и отпусканием последней клавиши сочетания из n клавиш.

Образ пользователя имеет ряд параметров, каждый из которых является случайной величиной. Совокупность значений одного параметра для каждого конкретного текста назовем вектором. Почерк является психологической характеристикой, и поэтому можно утверждать, что распределение его параметров в общем случае нормально[4].

Для проверки нормальности распределения существует целый ряд критериев. В данной работе для проверки нормальности распределения использован критерий Жака–Бера. Выбор данного критерия обусловлен тем, что обычно применяемые критерии дают большие погрешности на выборках малой длины[5].

Для проверки нормальности распределения по критерию Жака–Бера используется тот факт, что у нормального распределения коэффициент асимметрии равен нулю, а эксцесс равен 3, отклонение этих величин от нормальных значений служит мерой отклонения распределения от нормального. На основе выборки из параметров строится статистика Жака–Бера:

$$JB = \frac{T-k}{6}\left(S^2 + \frac{(K-3)^2}{4}\right), \qquad (1)$$

где T – количество наблюдений;

k – количество оцениваемых в модели параметров;

K – эксцесс;

S – коэффициент асимметрии.

В случае если распределения всех параметров будут нормальными, то для сравнения двух образов клавиатурного почерка возможно применение t-критерия Стьюдента.

Если нет уверенности в нормальности исследуемых распределений, имеет смысл обратиться к непараметрическому тесту – U-критерию Манна–Уитни[6].

Проведя ряд экспериментов, мы установили, что многие распределения параметров образа пользователя не являются нормальными. Таким образом, использование t-критерия Стьюдента невозможно.

Алгоритм сравнения образов пользователей

Сначала строится пересечение[7] сравниваемых образов. В результате в обоих образах остаются только общие параметры (буквы и n-граммы). Далее удаляются те параметры, векторы которых насчитывают менее пяти значений[8]. Затем для каждой пары параметров образов проверяется равенство медиан и вычисляется общее количество пар, у которых медианы совпадают. Итогом теста являлось число $K = Y_m / n$, где Y_m – число пар элементов, медианы которых не совпали, а n – общее количество параметров в сравниваемых образах. Назовем K коэффициентом различия образов пользователей.

Таким образом, используя описанный выше алгоритм, получаем степень численного различия двух образов, на основании которого возможна идентификация пользователя.

Экспериментально были установлены следующие границы для коэффициента различия образов пользователей.

$K \leq 0{,}2$ – образы принадлежат одному пользователю с уровнем достоверности 3σ.

$K \geq 0{,}2$ – образы принадлежат разным пользователям с уровнем достоверности 3σ.

Ошибки процедуры идентификации

На корректность процедуры идентификации пользователя по клавиатурному почерку приведенным выше методом влияют недостаточная длина текста; различные тексты; оборудование и программное обеспечение.

Таблица

Экспериментальные ошибки первого и второго рода для различных методов сравнения параметров клавиатурного почерка

	Один текст, одинаковое оборудование		Один текст, разное оборудование		Разные тексты, одинаковое оборудование		Разные тексты, разное оборудование	
Ошибка / Метод сравнения образов	1-го рода	2-го рода	1-го рода	2-го рода	1-го рода	2-го рода	1-го рода	2-го рода
Расстояние Эвклида	0,12	0,014	0,75	0,27	0,67	0,24	0,8	0,39
Коэффициенты корреляции Спирмена и Пирсена	0,09	0,007	0,24	0,11	0,15	0,05	0,56	0,13
U-критерий Мана–Уитни.	0,01	0	0,06	0	0,04	0	0,09	0,008

Различные тексты имеют различное частотное распределение букв и сочетаний, что ведет к сокращению параметров образов при построении пересечения. Таким образом, это усложняет задачу идентификации. Очевидно, что это практически не влияет на «короткие»[9] параметры, но оказывает заметное воздействие на длинные сочетания букв, которые могут серьезно различаться для двух текстов, на которых происходит сравнение почерка. Все эти факторы ведут к появлению ошибок.

Экспериментально установленные ошибки первого и второго рода для описанных выше методов сравнения двух образов клавиатурного почерка представлены в таблице.

Предложенный в настоящей работе подход позволил перехватывать символы, вводимые не только с физической клавиатуры, но и при использовании экранных клавиатур. Также опытным путем было установлено, что антивирусные приложения (в том числе работающие в режиме контроля реестра ОС и динамического контроля состояния системы) не классифицируют работу данного программного комплекса как потенциально опасный процесс, что

связано с использованием штатных функций ОС семейства Windows, предназначенных для обработки системных сообщений. Таким образом, становится возможной доработка модуля для решения задачи незаметного для пользователя процесса идентификации.

Заключение

Проведен сравнительный анализ возможности использования статистических критериев для решения актуальной задачи идентификации пользователя по его клавиатурному почерку. Доказана корректность выбора критерия Жака–Бера для сравнения образов почерков пользователей.

Разработан программный комплекс, способный идентифицировать пользователя по его работе с клавиатурой. В результате проведения ряда экспериментов по идентификации пользователей в различных условиях было установлено, что вероятность успешной идентификации пользователя при использовании данного комплекса составляет не менее 0,91.

Проведенные эксперименты показывают, что применение данного метода позволяет решить задачу незаметной идентификации пользователя. Также показано, что созданный комплекс позволит в будущем изменять как методы сбора данных, так и методы сравнения образов почерков, что существенно повышает эксплуатационную гибкость данного комплекса.

Исходя из результатов, представленных в данной работе, сделан вывод, что идентификация по клавиатурному почерку является актуальной и перспективной темой, требующей многоаспектного исследования возможности использования для этой задачи биометрических методов. Дальнейшие разработки, возможно, сделают идентификацию по клавиатурному почерку столь же распространенной процедурой, как и графологическая идентификация по рукописному почерку. Такой подход в перспективе может стать еще одним надежным инструментом выявления попыток НСД к защищаемым информационным ресурсам.

Примечания

[1] См.: *Иванов А.И.* Нейросетевые алгоритмы биометрической идентификации личности. М.: Радиотехника, 2004. 143 с; См.: ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». [Электронный ресурс] [М., 2006] URL: http://faculty.ifmo.ru/csd/files/52633-2006.pdf (дата обращения: 06.02.2012); См.: *Трушин Е.А.* Идентификация пользователя ЭВМ по клавиатурному почерку как метод защиты от несанкционированного доступа. [Электронный ресурс] [М., 1997] URL: http://www.securityclub.ru/ (дата обращения: 06.02.2012).

[2] См.: *Иванов А.И.* Указ. соч.

[3] См.: ГОСТ Р 52633-2006.

[4] См.: *Сидоренко Е.В.* Методы математической обработки в психологии. СПб., 2002. 350 с.

[5] См.: *Fay M.P., Proschan M.A.* Wilcoxon-Mann-Whitney or t-test? On assumptions for hypothesis tests and multiple interpretations of decision rules // Statistics Surveys. 2010. № 4. P. 1–39.

[6] См.: *Mann H.B., Whitney D.R.* On a test of whether one of two random variables is stochastically larger than the other // Annals of Mathematical Statistics. 1947. № 18. P. 50–60.

[7] Здесь имеется в виду пересечение в смысле множеств.

[8] См. требования критерия Мана–Уитни.

[9] Буквы и сочетания из двух и трех букв.

А.Н. Королев, А.А. Тарасов

О ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ НАВИГАЦИОННО-ИНФОРМАЦИОННЫХ СИСТЕМ

В статье рассмотрен подход к описанию структурной организации навигационно-информационных систем с точки зрения их функциональной устойчивости. Определены критерий, границы и запасы функциональной устойчивости навигационно-информационных систем. Сформулированы основные стратегии реконфигурации навигационно-информационных систем при деструктивных воздействиях на них с целью обеспечения автоматического восстановления их работоспособности.

Ключевые слова: навигационно-информационная система, функциональная устойчивость, навигационное поле, деструктивное воздействие, функциональная реконфигурация.

Широкое применение глобальных навигационных систем, прежде всего спутниковых систем радионавигации GPS и ГЛОНАСС, в последнее десятилетие привело к созданию и развитию целого класса информационных систем, предназначенных для обработки пространственно-временных и иных данных, основой которых служит навигационная и телеметрическая информация. Такие системы обычно называют навигационно-информационными системами (НИС).

НИС имеют специфические особенности построения (рис. 1).

К таким особенностям прежде всего следует отнести наличие обязательного элемента НИС – подсистемы определения местоположения объекта контроля. В эту подсистему входят специальные технические средства определения местоположения и параметров движения объекта контроля в пространственно-временном базисе, взаимодействующие с навигационным полем.

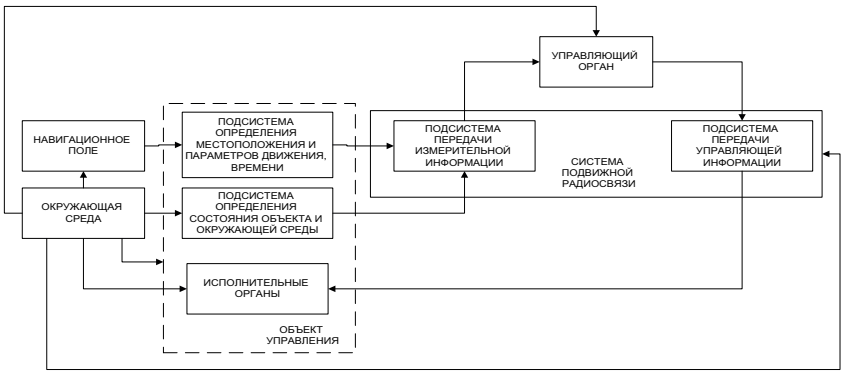


Рис.1. Обобщенная структура навигационно-информационной системы

Навигационные поля могут быть естественного или искусственного происхождения. К естественным навигационным полям можно, например, отнести магнитное и гравитационное поля Земли. В этих случаях навигационное поле строится как поле пространственно распределенных аномалий (гравитационных или магнитных), измерение которых соответствующими датчиками, установленными на объекте, дают информацию о текущем местоположении объекта. Другим примером естественных навигационных полей можно считать построение инерциального базиса в пространстве для использования методов инерциальной навигации или астронавигацию по картам звездного неба. К преимуществу использования естественных навигационных полей относится отсутствие затрат на их создание и поддержание, к недостаткам – низкая точность (поля гравитационных или магнитных аномалий), низкая доступность (астронавигация), накопление ошибок (инерциальная навигация).

В отличие от естественных навигационных полей, искусственные навигационные поля формируются специальными навигационными системами. По способу базирования выделяют спутниковые и наземные навигационные системы. По зоне действия – глобальные навигационные системы (ГНСС), системы ближней и дальней навигации. Искусственные навигационные поля, как правило, представляют собой зоны распространения навигационных радиосигналов, поэтому эти поля называют радионавигационными. Наибольшее распространение в настоящее время получили НИС, использующие радионавигационные поля ГНСС.

Этот факт обусловлен тем, что ГНСС ГЛОНАСС (РФ), GPS (США), а в ближайшей перспективе и Galileo (ЕС) обеспечивают глобальную зону покрытия (весь Земной шар), высокую точность и доступность. Еще одним немаловажным фактором является то, что ГНСС ГЛОНАСС и GPS обеспечивают бесплатный доступ к навигационным радиосигналам гражданского назначения.

Другая особенность НИС обусловливается необходимостью обмена информацией между подвижным объектом (объектами) контроля и управления и стационарным или подвижным органом (органами) управления. Это предполагает наличие в контуре управления системы подвижной радиосвязи, обеспечивающей телекоммуникационную среду обмена данными между объектом и субъектом управления в автоматизированной системе. Исключение составляют НИС, в которых объект и субъект управления пространственно объединены; это так называемые системы автономной навигации (автонавигаторы).

Некоторые современные системы подвижной радиосвязи, такие как сети мобильной связи GSM, CDMA и т. п., могут также являться источником радионавигационного поля, позволяющего наряду с задачей передачи данных решать и задачу местоопределения объектов контроля с определенным уровнем точности.

Следует заметить, что в отличие от задачи местоопределения объекта контроля и управления, задача определения параметров состояния объекта и окружающей среды не является обязательной для любого класса НИС. В простейшем случае измерительная подсистема НИС может ограничиваться только определением местоположения объекта.

Таким образом, НИС представляет собой многообъектную распределенную иерархическую систему автоматизированного управления. При этом сами объекты управления НИС изменяют во времени под действием внешних воздействий и внутренних факторов не только свое состояние, но и местоположение в пространстве, что влечет за собой, вследствие пространственных неоднородностей телекоммуникационной подсистемы и навигационного поля, изменения структурно-функциональных связей внутри самой системы. Кроме того, воздействие внешней среды (преднамеренное или непреднамеренное) на элементы системы может существенно влиять на ее работоспособность. В связи с этим необходима способность сохранять или восстанавливать (полностью или частично) возможность выполнения возложенных на нее функций в условиях воздействия деструктивных фак-

торов. Такую способность будем трактовать как функциональную устойчивость НИС[1]. Рассмотрим подход к описанию структурной организации НИС точки зрения обеспечения их функциональной устойчивости.

Пусть цель функционирования НИС состоит в реализации определенного набора функций

$$F = < f_1, f_2, .., f_n >. \quad (1)$$

Реализация каждой функции НИС на определенном интервале времени может выполняться с некоторым уровнем качества в зависимости от выделенных ресурсов системы для выполнения данной функции, изменения пространственного расположения объектов системы, состояния навигационного и связного полей и воздействий внешней среды в рассматриваемый интервал времени.

Рассмотрим $V = \{v_i\}$, $L = \|V\|$ – множество объектов управления НИС, каждый из которых характеризуется набором навигационных параметров $r(t)$ (координаты, скорость, направление движения и т. п.) в текущий момент времени t. Набор $R(t) = < r_1(t), r_2(t), .., r_L(t) >$ определяет пространственное положение объектов управления НИС в момент времени t. Основными характеристиками[2] навигационного поля в некотором месте пространства, входящем в рабочую зону системы навигации, являются точность навигационно-временных определений, целостность и доступность. В зависимости от этих характеристик навигационного поля в точке местоположения i-го объекта управления НИС измерения вектора могут быть произведены с различной степенью точности и достоверности. Например, если объект контроля находится на открытой местности и имеет возможность принимать как сигналы спутников ГНСС ГЛОНАСС/GPS, так и корректирующую информацию с геостационарных спутников широкозонных дифференциальных систем SBAS (WAAS, EGNOS, СДКМ и т. п.), то погрешность определения текущего местоположения объекта может быть не более 1 м. Если же объект находится на закрытой территории (например, в условиях городской застройки) и не имеет возможности принимать сигналы SBAS, то погрешность определения текущего местоположения может быть не менее 10 м. В случае невозможности определения местоположения по сигналам ГНСС, но нахождения объекта в зоне действия сети мобильной связи GSM погрешность определения его текущего местоположения может составить от нескольких десятков метров до не-

скольких километров. Таким образом, для каждой точки возможного расположения объектов контроля НИС можно определить потенциальный уровень качества пространственно-временной идентификации объекта (точность и достоверность оценки определения местоположения и параметров движения объекта). Если $\Phi = \{\varphi_i\}$– множество навигационных систем, по которым НИС имеет техническую возможность осуществлять пространственно-временную идентификацию своих объектов контроля, $X_N = \{x_i^N\}$ – множество областей в четырехмерном координатно-временном пространстве перемещения объектов контроля НИС, внутри каждой из которых характеристики навигационных полей постоянны, то имеет место следующее отображение:

$$\psi : \Phi \times X_N \to E, \tag{2}$$

где $E = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_N\}$ – упорядоченное конечное множество уровней качества пространственно-временной идентификации объектов контроля в НИС.

Поскольку системы подвижной связи, функционально входящие в НИС, формируют в пространстве перемещения объектов контроля НИС связные поля, характеризуемые пропускной способностью, доступностью и непрерывностью, то по аналогии с навигационными полями для каждой точки возможного расположения объектов контроля НИС можно определить потенциальный уровень качества информационного обмена (полнота, достоверность и задержка в передаче информации от объекта и к объекту). Пусть $H = \{\eta_i\}$ – множество систем связи, по которым НИС имеет техническую возможность осуществлять информационный обмен со своими объектами контроля, $X_i = \{x_i{}^C\}$ – множество областей в четырехмерном координатно-временном пространстве перемещения объектов контроля НИС, внутри каждой из которых характеристики связных полей постоянны, тогда имеет место следующее отображение:

$$\psi : H \times X_N \to \Gamma, \tag{3}$$

где $\Gamma = \{Y_1, Y_2, ..., Y_L\}$ – упорядоченное конечное множество уровней качества информационного обмена в НИС.

Пусть $Z = \{z_i\}$ – множество аппаратно-программных средств (АПС) НИС. Тогда для каждой функции f_i имеет место следующее отображение:

$$\omega_i : \mathrm{Z} \times \mathrm{E} \times \mathrm{X} \to Q^i, \tag{4}$$

где $Q^i = \{q_1^i, q_2^i, ..., q_{K_i}^i\}$ – упорядоченное конечное множество уровней качества реализации i-й функции. Для реализуемого НИС набора функций F существует множество Q уровней качества функционирования НИС, состоящее из непересекающихся подмножеств $\{Q^1, Q^2, ..., Q^N\}$ с элементами $q_j^i \in Q^i$, $i = \overline{1, N}$, упорядоченными согласно условию

$$q_1^i \le q_2^i \le ..., \le q_{K_i}^i, \; i = \overline{1, N} \tag{5}$$

Множество Q является частично упорядоченным и его удобно записывать в виде квазиматрицы[3] N-го порядка со строками – упорядоченными множествами Q^i:

$$Q = \left\| \begin{matrix} q_1^1 & \cdots & q_K^1 \\ \vdots & \ddots & \vdots \\ q_1^N & \cdots & q_{K_N}^N \end{matrix} \right\| = \; q_j^i \;, i = \overline{1, N}, j = \overline{1, K_i} \tag{6}$$

На множестве Q построим множество векторов

$$A = \{A_j\}, A_j = \{a_i^j\}, a_i^j \in Q^i, i = \overline{1, N}, j = \overline{1, M}, M = \prod_{i=1}^{N} K_i \tag{7}$$

где каждый вектор определяет некий уровень качества реализации набора функций F НИС.

На множестве векторов А введем *частичный* порядок

$$A_i \ge A_j \; : \forall \; (A_i \ni a_l^i = q_{k_l}^l \,, A_j \ni a_l^j = q_{m_l}^l \,, l = \overline{1, N}) \; (k_i \ge m_l) \tag{8}$$

и метрику

$$\begin{aligned} &\forall \; (A_i \,, A_j \in A, A_i \ge A_j) \;\; d(A_i \,, A_j) = \min_l \; (k_l - m_l), \\ &A_i \ni a_l^i = q_{k_l}^l \,, A_j \ni a_l^j = q_{m_l}^l \,, l = \overline{1, N} \end{aligned} \tag{9}$$

Пусть $Z^i \in Z$ – подмножество работоспособных аппаратно-программных средств (АПС) НИС, участвующих в реализации i-й функции НИС. Тогда существует некая конфигурация аппаратно-

программных средств (ресурсов) НИС для реализации набора функций F

$$k_l = < \mathrm{Z}_l^1, \mathrm{Z}_l^2, ..., \mathrm{Z}_l^N >, \mathrm{Z}_l^i \quad \mathrm{Z}, k_l \in K, i = \overline{1, N}, l = \overline{1, K}, \qquad (10)$$

причем множества АПС НИС Z_l^i являются пересекающимися, так как одни и те же АПС могут быть задействованы для реализации различных функций одновременно. На множестве K также можно ввести метрику, определяющую расстояние между распределениями k_l

$$d(k_i, k_j) = \sum_n \| (Z_i^n \cup Z_j^n) \setminus (Z_i^n \cup Z_j^n) \|, n = \overline{1, N}. \qquad (11)$$

Учитывая (4), можно утверждать, что каждой конфигурации аппаратно-программных средств (ресурсов) НИС k_l при определенных уровнях качества пространственно-временной идентификации объектов контроля ε_k и информационного обмена γ_m в НИС соответствует определенный уровень качества реализации набора функций A_j

$$\forall (k_l \in K, \gamma_m \in \Gamma, \varepsilon_k \in \mathrm{E}), \exists A_j \in : < k_l, \gamma_m, \varepsilon_k > \Rightarrow A_j, \qquad (12)$$

при этом один и тот же уровень качества реализации набора функций F НИС A_j может достигаться при различных конфигурациях аппаратно-программных средств k_l.

Для каждой i-й функции существует минимально допустимый уровень качества ее реализации $q_{r_i}^i$, при котором достигается цель функционирования НИС. Если система не способна обеспечить выполнение i-й функции с уровнем качества $q_{r_i}^i$ или выше, то считается, что i-й функция не выполняется системой. Введем вектор $A_{\lim}$, определяющий минимально допустимый уровень качества реализации набора функций F НИС

$$A_{\lim} = \{a_i^{\lim}\}, a_i^{\lim} = q_{r_i}^i, i = \overline{1, N}. \qquad (13)$$

Пусть $R = \{r_i\}$ – множество возможных деструктивных воздействий на НИС, вызывающих нарушения в ее работе. Тогда, используя выражения (11) и (12), можно формализовать понятие функциональной устойчивости НИС.

Определение. НИС является функционально устойчивой, если после деструктивного воздействия $r_i \in R$ существует хотя бы

одна работоспособная конфигурация аппаратно-программных средств (ресурсов), обеспечивающая реализацию набора функций F с уровнем качества не ниже $A_{\lim}$

$$\forall(k_l \in K, \gamma_m \in \Gamma, \varepsilon_k \in \text{E}), \exists k_l(r_i) \in K, < k_l, \gamma_m, \varepsilon_k > \Rightarrow A_{k_i}, A_{k_i} \geq A_{\lim}. \quad (14)$$

Уровень качества $A_{\lim}$ можно трактовать как границу устойчивости НИС к деструктивным воздействиям из R, а расстояние $d(A_{\lim}, A_{k_i})$ – как запас функциональной устойчивости НИС для конфигурации аппаратно-программных средств (ресурсов) k_l. При этом функциональная устойчивость НИС при деструктивных воздействиях обеспечивается функциональной перестройкой системы, включая:

– идентификацию после деструктивного воздействия на НИС состояния работоспособности ее аппаратно-программных средств (ресурсов) с учетом текущего распределения их $k_{тек}$ для реализации заданного набора функций;

– поиск конфигурации аппаратно-программных средств (ресурсов) НИС $k_{доп}$, обеспечивающей приемлемое качество реализации заданного набора функций в соответствии с (14);

– закрепление заданного набора функций НИС за программно-аппаратными средствами в соответствии с найденной конфигурацией $k_{доп}$.

Существуют различные стратегии функциональной перестройки. Они определяются такими требованиями к функциональной устойчивости, как:

– минимизация дополнительного оборудования, обеспечивающего функциональную устойчивость системы;

– минимизация времени восстановления работоспособности после деструктивного воздействия;

– максимальная адаптация системы к потоку деструктивных воздействий.

В зависимости от перечисленных требований можно выделить следующие стратегии ее функциональной перестройки.

1. Стратегия пригодности. Поиск осуществляется до нахождения первой конфигурации $k_{доп}$, удовлетворяющей условию

$$k_{доп} \in K, < k_{доп}, \gamma_m, \varepsilon_k > \Rightarrow A_{k_{доп}}, A_{k_{доп}} \geq A_{\lim}. \quad (15)$$

2. Стратегия максимального быстродействия при восстановлении работоспособности. Осуществляется поиск конфигурации $k_{доп}$, минимально отличающейся от текущей

$$d(k_{тек} - k_{доп}) = \min d(k_{тек} - k_i),\ \forall k_i \in K,\ A_{k_i} \geq A_{\lim}. \quad (16)$$

3. Стратегия максимального запаса функциональной устойчивости. Осуществляется поиск конфигурации $k_{доп}$, обеспечивающей максимальный запас функциональной устойчивости при текущем состоянии работоспособности аппаратно-программных средств (ресурсов) НИС

$$d(A_{\lim}, A_{k_{доп}}) = \min_i d(A_{\lim}, A_{k_i}),\ \forall k_i \in K,\ A_{k_i} \geq A_{\lim}. \quad (17)$$

Выбор той или иной стратегии осуществляется на этапе проектирования НИС.

Примечания

[1] См.: *Тарасов А.А., Бородакий Ю.В.* О функциональной устойчивости информационно- вычислительных систем // Известия. 2006. № 7.

[2] См.: ГОСТ Р 52865-2007. Глобальная навигационная спутниковая система. Параметры радионавигационного поля. М.: Стандартинформ, 2008. 23 с.

[3] См.: *Левин В.И.* Логическая теория надежности сложных систем. М.: Энергоатомиздат, 1985. 128 с.

С.В. Запечников, А.С. Полякова

ИССЛЕДОВАНИЕ МОДЕЛЕЙ ОЦЕНКИ ОПТИМАЛЬНОГО ОБЪЕМА ИНВЕСТИЦИЙ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

В настоящий момент организации нерационально вкладывают средства в обеспечение в информационной безопасности: до $^2/_3$ средств расходуются впустую. Недостаток принципов и рекомендаций по выбору оптимального объема инвестиций обусловливает необходимость выработки соответствующей методики оценки. В статье исследуется модель Гордона–Лоеба оценки оптимального объема инвестиций в информационную безопасность и модель взаимосвязанных рисков. Даются практические рекомендации по выбору и применению моделей, по выбору диапазона уязвимостей, на котором следует сосредоточить финансовые ресурсы, а также характеризуются слабые стороны моделей.

Ключевые слова: оптимальное инвестирование в информационную безопасность, модель Гордона–Лоеба, модель взаимосвязанных рисков.

Быстрое развитие компьютерных систем и сетевых технологий играет значительную роль в деятельности современных компаний. Поскольку эти системы все более и более интегрированы в бизнес-процессы, а нарушение их защищенности влечет за собой потери, и порой значительные, защита информационных активов становится критичной. В то время как нарастал объем исследований, связанных с технической стороной защиты информации (например, рассматривающих антивирусы, криптографические методы, аппаратные средства), появилось лишь небольшое количество работ, затрагивающих экономические аспекты информационной безопасности (ИБ). В настоящий момент организации нерационально вкладывают средства в обеспечение ИБ:

до $^2/_3$ средств расходуются впустую. Возрастающая необходимость защиты информационных активов, а значит, и инвестирования в эту защиту, а также недостаток принципов и рекомендаций по выбору оптимального объема инвестирования обусловливают необходимость исследования экономических аспектов безопасности информации и выработки методики оценки оптимального объема инвестиций в ИБ. Данная статья будет интересна менеджерам, отвечающим за распределение средств на обеспечение безопасности информации организаций, поскольку дает им практические рекомендации по выбору оптимального объема средств для инвестирования в ИБ.

Модель Гордона–Лоеба

Гордон и Лоеб[1] предложили экономическую модель, определяющую оптимальный объем инвестиций в ИБ для защиты заданного информационного ресурса. Модель рассматривает то, как уязвимость информации и потенциальные потери вследствие такой уязвимости влияют на оптимальный объем ресурсов, которые должны быть вложены в защиту информации нейтральной к риску организацией. Риски в данной модели считаются независимыми.

Информационный ресурс характеризуется тремя параметрами: λ, t, $\in [0,1]$, и $\nu \in [0,1]$, где λ – потери, обусловленные нарушением защищенности информации, t – вероятность возникновения угрозы, ν – уязвимость, определенная в модели как вероятность того, что реализованная угроза окажется успешной.

Хотя λ зависит от использования информации (самой организацией, конкурентами, хакерами) и меняется во времени, в модели рассматривается, что λ – фиксированное значение, конечное и меньшее некоторого очень большого числа M. Таким образом, модель не предназначена для случаев защиты национальных (государственных) активов или любых других, где потери могут быть катастрофическими. Для катастрофической потери $\lambda \geq M$ предположение о нейтральности к риску организации становится нереалистичным.

Для заданного информационного ресурса вероятность потери равна vt, а ожидаемая потеря, обусловленная отсутствием инвестиций в ИБ, равна $vt\lambda$. Таким образом, для любой положительной вероятности угрозы ($t > 0$) ожидаемая потеря возрастает с возрастанием уязвимости.

Для данной модели делается упрощение, что организация может инвестировать в уменьшение уязвимости, но не может влиять на уменьшение угроз. Поэтому вероятность угроз $t > 0$ фиксируется, и далее можно сфокусироваться на выборе объема инвестиций в целях уменьшения уязвимости. Поскольку $t = const$, определяется значение $L = t\lambda$ – потери или потенциальные потери, связанные с информационным ресурсом.

Вводится обозначение $z > 0$ – это денежные инвестиции в безопасность для защиты данного информационного ресурса. z измеряется в тех же единицах, что и потенциальные потери L. Целью инвестиции z является снижение вероятности нарушения защищенности информационного ресурса. Вводится $S(z, \upsilon)$ – *функция вероятности нарушения защищенности информационного ресурса* (ФВНЗИР) с уязвимостью υ, притом что организация инвестировала z в безопасность этого ресурса. Будем называть вероятностью нарушения защищенности значение функции $S(z, \upsilon)$ при заданных z и υ.

Для построения экономической модели Гордон и Лоеб предполагают, что функция $S(z, \upsilon)$ дважды непрерывно дифференцируема. Природа уязвимости и защищенности информации позволяет сделать следующие предположения касательно функции $S(z, \upsilon)$[2]:

Аксиома 1. $S(z, \upsilon) = 0$ для любых z . Если информационный ресурс абсолютно неуязвим, то он будет оставаться идеально защищенным для любого количества инвестиций z, включая нулевые.

Аксиома 2. $S(z, \upsilon) = 0$ для любых υ. При отсутствии инвестиций в информационную безопасность, вероятность нарушения защищенности информационного ресурса, обусловленная реализацией угрозы, является унаследованной от ресурса уязвимостью υ.

Аксиома 3. Для любых $\upsilon \in (0;1)$ и для любых z, $S_z(z, \upsilon) < 0$ и $S_{zz}(z, \upsilon) > 0$, где S_z – частная производная по z, а S_{zz} – частная производная Sz по z. Более того, согласно модели Гордона–Лоеба, предполагается, что для любых $\upsilon \in (0;1)$, $\lim S(z, \upsilon) \to 0$ при $z \to \infty$. Таким образом, при достаточном инвестировании в информационную безопасность вероятность нарушения защищенности информационного ресурса можно сколь угодно приблизить к нулю.

Далее считается, что ФВНЗИР удовлетворяет предположениям всех трех аксиом. С целью определения количества денежных средств для инвестирования в защищенность информации, организация сравнивает ожидаемую прибыль от инвестиций со стоимостью инвестиций. Ожидаемая прибыль от инвестиций в информационную безопасность, обозначенная через *EBIS*, равняется

уменьшению ожидаемых потерь организации, обусловленному дополнительной защитой:

$$EBIS\ (z) = [\upsilon - S(z, \upsilon)]L. \qquad (1)$$

Ожидаемая чистая прибыль от инвестиций в информационную безопасность, обозначенная через *ENBIS*, равняется разности *EBIS* и стоимости инвестиций:

$$ENBIS\ (z) = [\upsilon - S(z, \upsilon)]L - z.$$

Обозначим оптимальные инвестиции через $z^*(\upsilon)$.

Из аксиомы 3 следует, что $S(z, \upsilon)$ строго выпукла как функция от переменной z, а значит, *ENBIS* строго вогнута как функция от переменной z.

Для определения оптимального уровня инвестиций в ИБ решается задача поиска максимума функции:

$$ENBIS^*(z) = ENBIS(z^*) = max_z[\upsilon - S(z, \upsilon)]L - z.$$

Отсюда максимум $z^*(\upsilon) > 0$ находится из условия равенства нулю первой производной:

$$-S_z(z^*, \upsilon)L = 1,$$

где левая часть представляет собой предельную прибыль от инвестиций, а правая – предельную стоимость инвестиций. Необходимо инвестировать в безопасность только до той точки, где предельная прибыль от инвестиций равняется предельной стоимости инвестиций.

Для заданного уровня уязвимости оптимальный объем инвестиций в информационную безопасность z^* возрастает с возрастанием угрозы t или потерь λ.

Оптимальный объем инвестиций в ИБ проиллюстрирован на рис. 1. Из уравнения (1) и аксиом 1 и 2 следует, что прибыль от инвестиций $ENBIS(z)$ начинается в нуле и достигает υL с возрастанием уровня инвестиций. Стоимость инвестиций z показана с помощью прямой, составляющей угол 45° с осью z. Оптимальный объем инвестиций z^* находится там, где разница между прибылью и затратами максимальна. В этой точке касательная к $ENBIS(z^*)$ имеет тангенс угла наклона, равный 1, что свидетельствует о том, что предельная прибыль равна предельной стоимости.

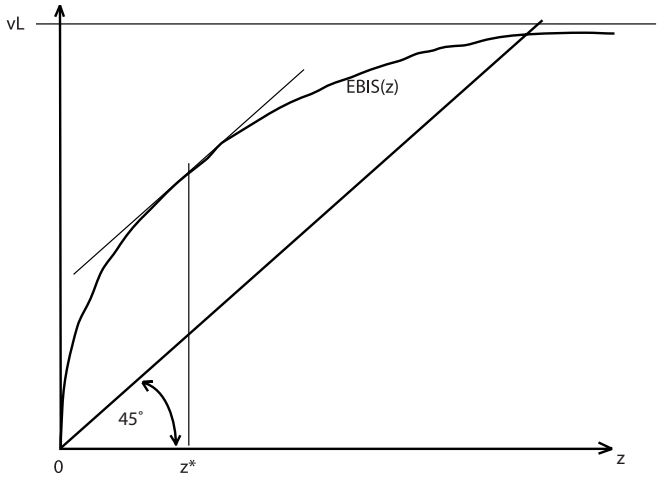


Рис. 1. Прибыль и стоимость инвестиций
в информационную безопасность

Оптимальный объем инвестиций в ИБ равняется нулю, если предельная прибыль при $z = 0$ меньше или равняется предельной стоимости такой инвестиции. Это условие может быть записано в виде:

$$L \le 1/(-S_z(0, \upsilon)).$$

Исследуются два широких класса функций $S(z, \upsilon)$.

Первый класс, обозначенный через $S^I(z, \upsilon)$, задается как

$$S^I(z, \upsilon) = \upsilon/((\alpha z + 1)^{\beta}),$$

где параметры $\alpha > 0$, $\beta \ge 1$ – меры эффективности ИБ. ФВНЗИР этого класса линейны по уязвимости. Рис. 2 показывает, как возрастание инвестиций в ИБ, z, уменьшает ожидаемую потерю от нарушения защищенности информационного ресурса. Разница между значениями, которые принимают линейные функции вида $S(z, \upsilon)L$ в точке υ, и представляет собой *ENBIS*.

Выражение для оптимального уровня инвестиций в ИБ для $S^I(z, \upsilon)$ имеет вид:

$$z^{I^*}(\upsilon) = ((\upsilon\beta\alpha L)^{1/(\beta+1)} - 1)/\alpha).$$

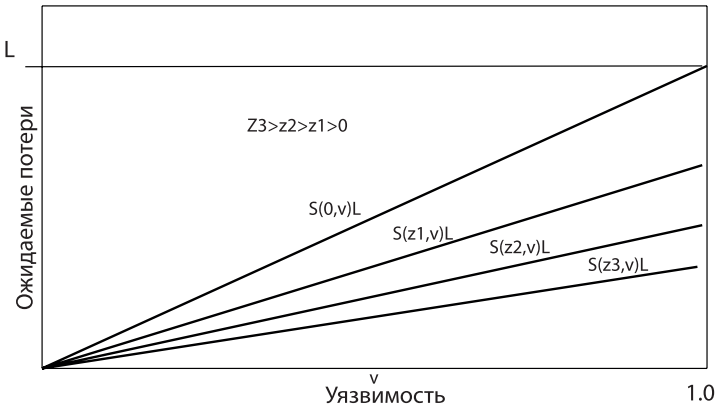


Рис. 2. Ожидаемый объем потерь, $S(z, \upsilon)L$ при увеличении уязвимости, а также при разных уровнях инвестиций в ИБ для первого класса ФВНЗИР

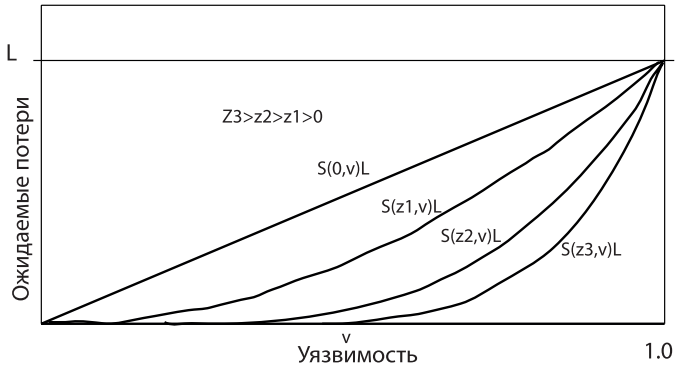


Рис. 3. Величина ожидаемых потерь $S(z, \upsilon)L$ при увеличении уязвимости, а также при разных уровнях инвестиций в ИБ для второго класса ФВНЗИР

Второй класс ФВНЗИР задается в виде $S^{II}(z, \upsilon) = \upsilon^{\alpha z+1}$, где параметр $\alpha > 0$ – мера эффективности ИБ. Каждая кривая на рис. 3 представляет собой функцию, принадлежащую классу $S^{II}(z, \upsilon)$.

Выражение для оптимального уровня инвестиций в ИБ имеет в вид:

$$z^{II*}(\upsilon) = ln(1/(-\alpha\upsilon L(ln\ \upsilon)))/\alpha\, ln\upsilon\,.$$

Гордон и Лоеб доказывают, что для ФВНЗИР, принадлежащих первому или второму классу, оптимальный уровень инвестиций никогда не превосходит величины 1/e = 36,79% от ожидаемых потерь. Для широкого круга функций, принадлежащих первому и второму классам, оптимальный объем инвестиций в ИБ значительно меньше максимума 36,79%.

Для первого класса ФВНЗИР оптимальный уровень инвестиций в ИБ возрастает с увеличением уязвимости ресурса, а для второго класса ФВНЗИР оптимальный уровень инвестиций в ИБ сначала возрастает с увеличением уязвимости ресурса, а затем убывает. Таким образом, второй класс ФВНЗИР показывает, что менеджерам стоит концентрировать финансовые ресурсы на защите информации в диапазоне средней уязвимости.

В исходную формулировку модели Гордона–Лоеба можно внести уточнения и расширить ее.

Джен Уиллемсон (Jan Willemson) в своей работе[3] показывает, что аксиома 3 выполняется не всегда: из неравенства $S_z(z, \upsilon) < 0$ следует, что если вначале полагалось $\upsilon = 0$, то невозможно уменьшить вероятность атаки строго до нуля независимо от того, насколько большой объем инвестиций вкладывается в ИБ. Хотя это и может служить хорошим приближением для многих реальных ситуаций, но совершенно точно существуют угрозы, которые могут быть полностью устранены достаточным инвестированием в меры ИБ. Он приводит уточнение этой аксиомы и формулирует аксиому 3': Функция $S(z, \upsilon)$ дважды непрерывно дифференцируема и

$$S_z(z, \upsilon) \leq 0 \text{ и } S_{zz}(z, \upsilon) \geq 0,$$

а также для любых υ, $lim\ S(z, \upsilon) \to 0$ при $z \to \infty$.

Далее путем конструирования специального класса функций, удовлетворяющих аксиомам 1, 2, 3', Уиллемсон показывает, что оптимальный объем инвестиций достигает 50% ожидаемой потери в отсутствие инвестиций в ИБ (в отличие от 36,79 в модели Гордона–Лоеба). Также Уиллемсон показал, что если убрать условие непрерывности второй производной ФВНЗИР, то можно получить уровень оптимальных инвестиций в ИБ, близкий к 100% от ожидаемых потерь. Возможность убрать это условие он обосновывает тем, что непрерывность первой производной необходима для существования второй производной, но по существу нет причин для второй производной быть непрерывной.

Также Уиллемсон отмечает[4] необходимость условия монотонности ФВНЗИР по υ. В противном случае для некоторой инвестиции z можно найти такие начальные уровни уязвимостей $\upsilon_1 < \upsilon_2$, что после инвестирования z получим $S(z, \upsilon_1) > S(z, \upsilon_2)$. Это противоречит представлениям, однако аксиомы 1–3 не запрещают такой случай.

В аксиоме 3 прописано ограничение $\upsilon < 1$. Иными словами, если изначально уровень уязвимости составляет $\upsilon = 1$ (любая атака будет успешной), то будет невозможно уменьшить эту уязвимость, какой бы объем ни был инвестирован в ИБ. Это противоречит общепринятым представлениям о защите информационного ресурса, поэтому стоит считать, что $\upsilon \in (0,1)$.

Модель взаимосвязанных рисков

В связи с тем что информационные системы интегрированы и взаимосвязаны, решения организации относительно инвестиций в ИБ затрагивают не только эти организации, но и другие. Свойство взаимосвязанности рисков информационной безопасности обусловливает различные внешние эффекты. Инвестиции в ИБ могут вызывать положительные внешние эффекты: организация, увеличивая свой уровень ИБ путем инвестирования в технические решения, может снизить вероятность нарушения защищенности других организаций-партнеров через компьютерную сеть. Напротив, внешние эффекты могут быть и отрицательными: возросший уровень ИБ организации может перенаправить атаки злоумышленников с высокозащищенного сервера на менее защищенные серверы, а значит, риски других организаций возрастают. Отсюда в случае положительных внешних эффектов организация, вероятно, будет инвестировать меньшую долю от ожидаемых потерь в отсутствие инвестиций в ИБ, а в случае отрицательных – бóльшую. В первом случае имеем нецелевые атаки, во втором – целевые.

Вухен Шим[5] показывает, что инвестиции, направленные на борьбу с нецелевыми атаками, призванными навредить как можно большему числу уязвимых систем, вызовут положительные внешние эффекты, поскольку возросшие инвестиции организации снизят риски для других организаций, связанных с данной системой. Он также показал, что инвестиции, направленные на борьбу с целевыми атаками, призванными причинить ущерб конкретной компьютерной системе, вызовут отрицательные внешние эффекты, поскольку возросшие инвестиции организации перенаправят

Рис. 4. Связи между типами атак и внешними эффектами

атаки на другие организации и тем самым увеличат риски других организаций. Связи между типами атак и проблемой внешних эффектов показаны на рис. 4.

Шим разработал модель взаимосвязанных рисков, расширяющую модель Гордона–Лоеба. Он рассматривает два класса ФВНЗИР, представленные Гордоном и Лоебом, при условии взаимосвязанности рисков. Пусть L_i, υ_i, z_i, $S_i(z_i, \upsilon_i)$ – потенциальные потери, уязвимость, инвестиции в ИБ и ФВНЗИР i-й организации, соответственно. Для упрощения модели рассматриваются две идентичные организации ($i = 1, 2$), т. е. такие, что $z_1 = z_2$, $L_1 = L_2$, $\upsilon_1 = \upsilon_2$, $S_1(z_1, \upsilon_1) = S_2(z_2, \upsilon_2)$.

Для рассмотрения случая отрицательных внешних эффектов вводится z_1/z_2 – относительная эффективность инвестиций организации 1. Тогда

$$S_1^I(z_1, z_2, \upsilon_1) = \upsilon_1/[(\alpha \cdot (z_1 \cdot (z_1/z_2)) + 1)^{\beta}].$$

Предполагая, что организации 1 и 2 идентичны, имеем:

$$z_1^{I*}(\upsilon_1) = [(2\alpha ß \upsilon_1 L_1)^{1/(ß+1)} - 1]/\alpha.$$

Для случая отрицательных внешних эффектов

$$S_1^{II}(z_1, z_1, \upsilon_1) = \upsilon_1^{[\alpha \cdot (z1 \cdot (z1/z2)) + 1]}.$$

Оптимальный уровень инвестиций в случае идентичности организаций принимает вид:

$$z_1^{II*}(\upsilon_1) = ln[1/(-2\alpha \upsilon_1 L1(ln\ \upsilon_1))]/\alpha\ ln\ \upsilon_1.$$

Положительные внешние эффекты моделируются путем классификации эффектов на прямые и косвенные. Под прямыми эффектами имеется в виду влияние инвестирования организации на свою собственную ФВНЗИР, а под косвенными – влияние инвестирования других организаций на ФВНЗИР этой организации. Для моделирования косвенных эффектов используется параметр δ, показывающий степень взаимосвязанности информационных систем двух организаций ($0 \le \delta \le 1$). Чем выше δ, тем выше степень взаимосвязанности. Тогда ФВНЗИР для организации 1 может быть выражена так:

$$S_1^I(z_1, z_2, \upsilon_1) = p_1(z_1 + \delta z_2, \upsilon_1).$$

Отсюда

$$S_1^I(z_1, z_2, \upsilon_1) = \upsilon_1/[(\alpha \cdot (z_1 + \delta z_2)) + 1)^ß].$$

Предполагая, что организации 1 и 2 идентичны, имеем:

$$z_1^{I*}(\upsilon_1) = [(\alpha ß \upsilon_1 L_1)^{1/(ß+1)} - 1]/(\alpha(1 + \delta)).$$

ФВНЗИР второго класса имеют вид:

$$S_1^{II}(z_1, z_1, \upsilon_1) = \upsilon_1^{[\alpha \cdot (z1 + \delta z2)) + 1]}.$$

А оптимальный уровень инвестиций для идентичных организаций равен:

$$z_1^{II*}(\upsilon_1) = ln[1/(-\alpha \upsilon_1 L_1(ln\ \upsilon_1))]/\alpha(1 + \delta)\ ln\ \upsilon_1].$$

Сравнение моделей

Модель Гордона–Лоеба предназначена для оценки оптимального объема инвестиций в ИБ в случае независимых рисков. Модель взаимосвязанных рисков базируется на модели Гордона–Лоеба и является ее расширением для случая положительных и отрицательных внешних эффектов. При отрицательных внешних эффектах оптимальный объем инвестиций оказывается выше или равен оптимальному объему в модели с независимыми рисками, а область нулевых инвестиций оказывается меньше, чем в модели с независимыми рисками. При положительных внешних эффектах оптимальный объем инвестиций оказывается ниже или равен оптимальному объему в модели с независимыми рисками, а область нулевых инвестиций оказывается такой же, как в модели с независимыми рисками.

На рис. 5 и 6 показана зависимость оптимального объема инвестиций от уязвимости (черным цветом), а также изменение его при положительных и отрицательных внешних эффектах.

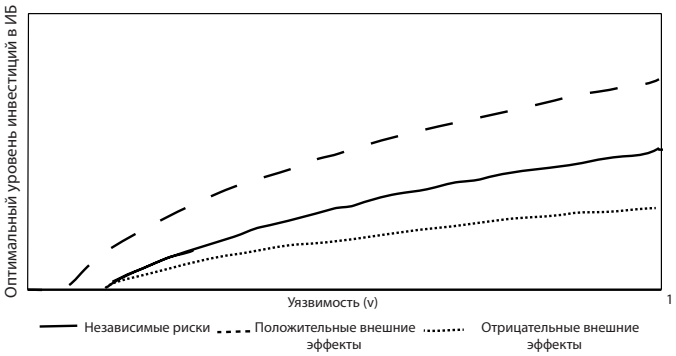


Рис. 5. Характерный вид графиков, показывающий оптимальный объем инвестиций в ИБ для первого класса ФВНЗИР в зависимости от типов рисков

В случае применения модели Гордона–Лоеба оптимальный объем инвестиций в ИБ не превышает 36,97% от ожидаемых потерь. В модели взаимосвязанных рисков с отрицательными внешними эффектами оптимальный объем инвестиций в ИБ не превосходит 73,56% от ожидаемых потерь. В модели взаимосвязанных рисков с положительными внешними эффектами оптимальный объем инвестиций в ИБ не превосходит $(1 + \delta)^{-1} \cdot 36{,}97\%$ от ожидаемых потерь.

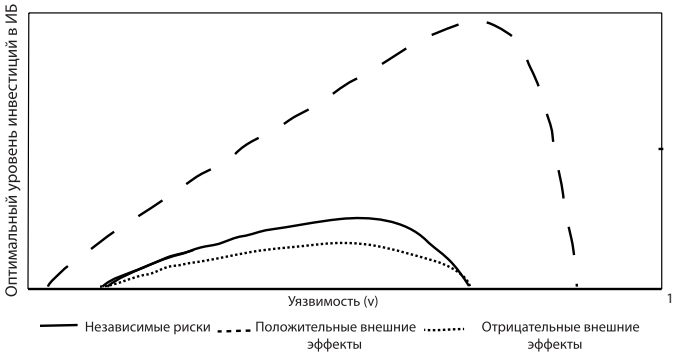


Рис. 6. Характерный вид графиков, показывающий оптимальный объем инвестиций в ИБ для второго класса ФВНЗИР в зависимости от типов рисков

При выборе той или иной модели прежде всего нужно решить, возможно ли пренебречь взаимосвязанностью рисков в данном конкретном случае. Для этого необходимо исследовать взаимодействие данной организации с другими, а также ее положение на рынке. Если положительные и/или отрицательные внешние эффекты существенны, то разумнее применение модели взаимосвязанных рисков. Положительные внешние эффекты существенны, когда несколько организаций связаны, например, компьютерной сетью. В этом случае инвестирование одной из организаций в свою информационную безопасность повлечет уменьшение уязвимости и второй организации. Отрицательные внешние эффекты существенны, когда велика вероятность того, что увеличение защищенности одной организации перенаправит атаки злоумышленников на рассматриваемую.

Однако модель взаимосвязанных рисков рассматривает идентичные организации, что далеко не всегда имеет место. В случае неидентичности организаций может возникнуть ситуация, когда внешними эффектами можно пренебречь. Например, состояние рынка таково, что на нем существует один безусловный лидер, обладающий информацией высокой ценности, и огромное количество приближенно идентичных между собой организаций, чьи продукты не столь хороши. Тогда отрицательный внешний эффект инвестиций в ИБ безусловного лидера на идентичные менее успешные организации минимизируется из-за большого числа этих организаций, поскольку вероятность перенаправления атаки

именно на эту организацию мала. В таком случае нет смысла использовать модель взаимосвязанных рисков и можно применить модели Гордона–Лоеба.

В табл. 1 приведена сравнительная характеристика модели Гордона–Лоеба и модели взаимосвязанных рисков.

Модель Гордона–Лоеба и модель взаимосвязанных рисков строятся на двух классах ФВНЗИР. Анализ первого класса говорит о том, что менеджерам стоит сосредоточивать свои финансовые ресурсы на информационных ресурсах большой уязвимости, в то время как анализ второго класса показывает необходимость инвестирования в ИБ информационных ресурсов среднего диапазона уязвимости. Можно аргументировать выбор одного из двух классов размерами ожидаемых потерь в случае отсутствия инвестирования в ИБ. Если информация чрезвычайной важности и ожидаемый ущерб велик, то разумнее выбрать первый класс ФВНЗИР и защищать высокоуязвимые ресурсы, дабы минимизировать потери. Но не стоит забывать, что модели не рассматривают случай катастрофичных потерь, поскольку в этом случае предположение о нейтральности к риску организации не подтверждается. В случае же, когда ожидаемый ущерб не столь велик, прибыть от инвестиций в защищенность высокоуязвимых ресурсов мала. Например, для случая конфиденциальности знание того, что организация продает определенный бизнес-модуль, может стать почти общедоступной. В этом случае из-за множественных источников потенциальной утечки информации будет слишком дорого контролировать персонал и бизнес-контакты, чтобы предоставить хотя бы базовый уровень ИБ. Следовательно, разумнее использовать второй класс ФВНЗИР и концентрировать финансовые ресурсы на защите информационных ресурсов из диапазона средней уязвимости.

У моделей есть и слабые стороны.

Модель Гордона–Лоеба содержит неточности, которые, однако, не влияют на выбор первого и второго класса ФВНЗИР. Вследствие незначительного ослабления условия в модели Гордона–Лоеба становится возможным построить пример, когда оптимальный объем инвестиций достигает 50% и даже 100% от ожидаемых потерь.

Обе модели базируются на двух специфических классах ФВНЗИР, и остается неясным, дадут ли другие классы функций похожие результаты.

Таблица 1

Сравнительная характеристика модели Гордона–Лоеба и модели взаимосвязанных рисков

Молель Гордона–Лоеба		Модель взаимосвязанных рисков	
Тип рисков	Независимые риски	Взаимосвязанные риски, порождающие либо положительные, либо отрицательные внешние эффекты на инвестиции организации в ИБ	
Верхняя граница оптимального объема инвестиций в ИБ	36,79% от ожидаемых потерь	Отрицательные внешние эффекты	73,58% от ожидаемых потерь
		Положительные внешние эффекты	$(1+\delta)^{-1} \cdot 36{,}97\%$ от ожидаемых потерь
Формула для расчета оптимального объема инвестиций для первого класса ФВНЗИР	$z^{I*}(\upsilon) = ((\upsilon ß \alpha L)^{1/(ß+1)} - 1)/\alpha)$, где параметры $\alpha > 0$, $ß \geq 1$ – меры эффективности ИБ	Отрицательные внешние эффекты	$z_1^{I*}(\upsilon_1) = [(2\alpha ß \upsilon_1 L_1)^{1/(ß+1)} - 1]/\alpha$. где параметры $\alpha > 0$, $ß \geq 1$ – меры эффективности ИБ
		Положительные внешние эффекты	$z_1^{I*}(\upsilon_1) = [(\alpha ß \upsilon_1 L_1)^{1/(ß+1)} - 1]/(\alpha(1+\delta))$ где $0 \leq \delta \leq 1$ – параметр, показывающий степень взаимосвязанности информационных систем двух организаций, параметры $\alpha > 0$, $ß \geq 1$ – меры эффективности ИБ
Формула для расчета оптимального объема инвестиций для второго класса ФВНЗИР	$z^{II*}(\upsilon) = ln(1/(-\alpha \upsilon L(ln\ \upsilon)))/\alpha \ln \upsilon$ где параметр $\alpha > 0$ – мера эффективности ИБ	Отрицательные внешние эффекты	$z_1^{II*}(\upsilon_1) = ln[1/(-2\alpha \upsilon_1 L_1(ln\ \upsilon_1))]/\alpha\ ln\ \upsilon_1$ где параметр $\alpha > 0$ – мера эффективности ИБ
		Положительные внешние эффекты	$z_1^{II*}(\upsilon_1) = ln[1/(-\alpha \upsilon_1 L_1(ln\ \upsilon_1))]/[\alpha\ (1+\delta)(ln\ \upsilon_1)]$ где $0 \leq \delta \leq 1$ – параметр, показывающий степень взаимосвязанности информационных систем двух организаций

Таблица 2

Сравнительная таблица расчетов оптимального объема инвестиций в ИБ для модели Гордона-Лоеба и модели взаимосвязанных рисков, а также для обоих классов ФВНЗИР и обоих типов внешних эффектов

Уязвимость	$z^{I*}(\upsilon)$, модель Гордона–Лоеба	$z^{II*}(\upsilon)$, модель Гордона–Лоеба	$z_1^{I*}(\upsilon_1)$, модель взаимосвязанных рисков, отрицательные внешние эффекты	$z_1^{I*}(\upsilon_1)$, модель взаимосвязанных рисков, положительные внешние эффекты	$z_1^{II*}(\upsilon_1)$, модель взаимосвязанных рисков, отрицательные внешние эффекты	$z_1^{II*}(\upsilon_1)$, модель взаимосвязанных рисков, положительные внешние эффекты
0,05	0,0	0,0	0,0	0,0	6038,5	0,0
0,1	0,0	0,0	16960,7	0,0	26530,6	0,0
0,15	6265,9	6826,7	33886,6	3685,8	43363,5	4015,7
0,2	16960,7	15703,7	47361,3	9976,9	58771,4	9237,5
0,25	25992,1	23561,7	58740,1	15289,5	73561,7	13859,8
0,3	33886,6	30561,2	68686,5	19933,3	88132,8	17977,2
0,35	40946,0	36681,7	77580,8	24085,9	102706,9	21577,5
0,4	47361,3	41753,3	85663,6	27859,6	117400,4	24560,8
0,45	53261,9	45431,7	93097,9	31330,5	132237,1	26724,6
0,5	58740,1	47123,4	100000,0	34553,0	147123,4	27719,6
0,55	63864,3	45835,3	106456,0	37567,2	161777,8	26961,9
0,6	68686,5	39884,8	112531,7	40403,8	175576,3	23461,6
0,65	73247,8	26315,0	118278,6	43087,0	187219,0	15479,4
0,7	77580,8	0,0	123737,8	45635,8	193968,3	0,0
0,75	81712,1	0,0	128942,8	48065,9	189744,2	0,0
0,8	85663,6	0,0	133921,4	50390,3	159699,0	0,0
0,85	89453,6	0,0	138696,6	52619,8	61507,8	0,0
0,9	93097,9	0,0	143288,1	54763,5	0,0	0,0
0,95	96609,5	0,0	147712,5	56829,1	0,0	0,0

Обе модели не учитывают динамические аспекты, а именно эффект инвестиций. В частности, не рассматривается, как злоумышленник меняет стратегии своих атак в ответ на дополнительные инвестиции в ИБ.

Существуют трудности в получении данных для обеих моделей, таких как количественные оценки ущерба, вероятности возникновения угроз и уязвимости.

Модель взаимосвязанных рисков разработана лишь для идентичных организаций, что не всегда имеет место.

В табл. 2 приведены результаты расчета оптимального объема инвестиций для конкретного случая. При этом берется: $\alpha = 0{,}00001$, $L = 400\,000$, $ß = 2$, $\delta = 0{,}7$. Расчет выполнен для обеих моделей оценки и для обоих классов ФВНЗИР.

Как следует из табл. 2, для данного случая оптимальный объем инвестиций в модели Гордона–Лоеба не превышает 25% от ожидаемых потерь, в модели взаимосвязанных рисков с отрицательными внешними эффектами оптимальный объем инвестиций не превышает 40% от ожидаемых потерь, в модели взаимосвязанных рисков с положительными внешними эффектами оптимальный объем инвестиций не превышает 14% от ожидаемых потерь.

Полученные результаты углубляют исследования экономических аспектов информационной безопасности, предоставляют практические рекомендации по выбору и применению моделей оценки объема оптимальных инвестиций в ИБ, а также по выбору диапазона уязвимостей, на котором следует сосредоточить ресурсы. Продолжение исследования может заключаться в разработке методики оценки оптимального уровня инвестиций, учитывающей динамические аспекты, а также конкретные области инвестирования, такие как программное или аппаратное обеспечение защищенных компьютерных информационных систем.

Примечания

[1] См.: *Gordon L.A.* The Economics of Information Security Investment / Gordon L.A., Loeb M.P. // ACM Transactions on Information and System Security. Vol. 5. No. 4. November 2002. P. 438–457.

[2] Ibid. P. 443.

[3] См.: *Willemson J.* On Gordon & Loeb Model for Information Security Investment. [Электронный ресурс]. [M.,2006]. URL: http://weis2006.econinfosec.org/docs/12.pdf (дата обращения: 02.02.2012).

[4] См.: *Willemson J.* Extending the Gordon&Loeb Model for Information Security Investment. [Электронный ресурс]. [M.,2010]. URL: http://research.cyber.ee/~jan/publ/aresGL.pdf (дата обращения: 02.02.2012).

[5] См.: *Shim W.* Vulnerability and Information Security Investment under Interdependent Risks: a Theoretical Approach // Asia Pacific Journal of Information Systems. 2011. No. 12. P. 27–43.

А.Е. Баранович, Д.Б. Ханковский

О МОДЕЛИРОВАНИИ ВЗАИМОДЕЙСТВИЯ ПОДПРОЦЕССОВ МЫШЛЕНИЯ УРОВНЕЙ «СОЗНАНИЕ»–«ПОДСОЗНАНИЕ»

В рамках информационно-эволюционного подхода к системному анализу и моделированию интеллектуальных систем исследуются механизмы взаимодействия подпроцессов мышления уровней «сознание»–«подсознание». Показана возможность построения биективного соответствия между моделями информационных объектов подпроцессов мышления различной этимологии. Тем самым формируются основы алгоритмической реализации взаимодействия моделей подпроцессов мышления различных уровней в антропогенно-технических системах «искусственного интеллекта». Статья продолжает цикл работ, посвященных моделированию универсальных механизмов интеллектуальной деятельности различного генезиса

Ключевые слова: информация, мышление, знания, интеллектуальные системы, сознание, подсознание

ВВЕДЕНИЕ

До последнего времени основное внимание в специализациях «Системный анализ» и «Математическое моделирование» предметной области «Прикладная математика» уделялось исследованию классов физических и кибернетических систем[1]. В настоящее время внимание сдвигается к исследованию сложных систем высшего порядка, а именно интеллектуальных систем, единственным актуально наблюдаемым представителем которых, является человек – антропная интеллектуальная система. Эволюция системных представлений в области теории интеллектуаль-

ных систем выдвинула к настоящему периоду следующую научную парадигму: базовые информационные процессы интеллектуальной деятельности (мышления) представляются двумя типами подпроцессов: сознательными (осознаваемыми) и подсознательными (неосознаваемыми субъектом – носителем интеллекта). Более того, указанные подпроцессы реализуют различные мыслительные функции. Предполагается, что на сознательном уровне реализуются логические алгоритмические вычисления (модели А. Тьюринга–Дж. фон Неймана), а на подсознательном – процессы алогического мышления (нелинейная динамика, нейродинамика, синергетика).

1. АКСИОМАТИКО-ТЕРМИНОЛОГИЧЕСКИЙ БАЗИС

Формулировка направления «Моделирование мышления»[2] требует весьма скрупулезного изложения и максимально строгого нетранзитивного определения понятий, задействованных в ней. Первое непосредственное составляющее (по Л. Блумфилду[3]): моделирование – понятие, с наших позиций не вызывающее существенных разночтений. Мы будем придерживаться следующего определения: *моделирование* (*фр.* modele – образец, прообраз) – воспроизведение характеристик некоторого объекта на другом объекте (*модель*[4]), специально созданном для их изучения; подобие между моделью и объектом может заключаться в сходстве физических характеристик модели и объекта, либо в сходстве функций, осуществляемых моделью и объектом, либо в тождестве математического описания «поведения» объекта и его модели[5].

В настоящей работе вводится определение *мышления*, основанное на аксиоматико-терминологическом аппарате информационно-эволюционного подхода (ИЭП) к системному анализу и моделированию (САМ) объективной реальности[6], включающем следующие термины-понятия[7].

Локус – фиксированная и вполне определенная ограниченная часть объективной реальности (ОР).

Система – совокупность элементов, связанных структурой, характеризуемая вполне определенной целостностью. Элементы системы есть *подсистемы.* Система есть элемент *надсистемы. Объект* есть подсистема, декларируемая неделимой на заданном уровне антропного моделирования.

Структура – строение и внутренняя форма организации системы, выступающая как единство устойчивых связей между ее элементами, а также законов данных взаимосвязей.

Система материальная (МС) – пространственно-временной локус[8], характеризуемый системной целостностью.

Система кибернетическая (КС) – телеологическая МС естественного или искусственного происхождения, характеризуемая наличием механизмов энергоинформационного *адаптивного управления*[9] собственным существованием во внешней среде.

Интеллект – способность развитых КС в процессе адаптивного управления собственным существованием во внешней среде оперировать индивидуально-имманентными информационными *моделями* ОР.

Система интеллектуальная (ИС) – КС, обладающая интеллектом (интеллектуальными свойствами). Последнее предполагает наличие в ИС вполне определенных подсистем знаний и принятия решений той или иной степени развития, включающих механизмы сенсориума, синтеза, анализа, хранения и пре образования моделей ОР (знаний различного уровня генезиса), а также механизмы выработки решений на управление ИС. В отношении классов МС, КС и ИС выполнимо соотношение: {ИС} ⊂ {КС} ⊂ {МС}.

Знания – структурированная совокупность (система) информационных моделей и метамоделей взаимодействующих материальных систем объективной реальности различного уровня генезиса, хранимая в соответствующей подсистеме интеллектуальной системы и используемая ею для организации эффективного адаптивного управления собственным существованием во внешней среде.

*Знания вербализованные (*лат. verbum – слово*)* – знания, сформированные в эволюционном процессе семантической коммуникации коллектива ИС с использованием аппарата семиотико-иконических конструкций естественного языка (ЕЯ). Вербализованным знаниям присущи вполне определенные ограничения на характеризацию ОР[10].

В представленной терминологической системе речь неоднократно идет об информации и процессах ее преобразования. Словоформа «информация» в работе представлена определением, базирующимся на совокупности шести постулатов атрибутивно-ингрдиентной концепции[11] (АИКИ), характеризующих восприятие авторами сущности декларированного понятия: «информация есть

фундаментальная категория[12] идентифицирующая неотъемлемый ингредиент[13] ОР, характеризующий *формы* ее бытия». Как следствие, «информация» в интерпретации «обыденного» языка в АИКИ преобразуется в ряд нетранзитивно связанных аксиоматических понятий, составляющих основу терминологического аппарата *информациологии*: «*информация*» (как результат), «*информационный прообраз*» как информационная составляющая формы реализации (существования) текущего состояния ОР (МС), «*информационный образ*» как информационная составляющая результата взаимодействия МС, воспринимаемая участвующими МС, «*информатизация*» как закономерно-имманентный процесс (естественно-имплицитный, антропогенный и т. п.) упорядоченной смены информационных форм ОР, «*информирование*» как процесс информационного взаимодействия МС.

В контексте вышеиспользованного аксиоматико-терминологического аппарата определим понятие «мышление» следующим образом.

Мышление – целенаправленный (информационный) *процесс* оперирования информационными моделями внешнего мира различного уровня генезиса, инициируемый ИС.

Абстрактное мышление, в свою очередь, есть имманентная характеристика мышления развитых ИС, заключающаяся в способности оперирования метамоделями объективной реальности различного уровня категоризации.

Мысль, соответственно, есть *результат* (фиксированное в «текущем настоящем», финальное либо промежуточное состояние) мышления[14].

2. АППАРАТ МОДЕЛИРОВАНИЯ

В используемом нами представлении информационное функционирование ИС реализуется в двух «плоскостях»: «сознание» и «подсознание». Стоит отметить, что в данной работе мы вполне осознанно не концентрируемся на интерпретации понятий «сознание» и «подсознание» с точки зрения психологии (хотя, в определенном смысле, предлагаемый подход и связан с моделированием некоторых психических актов). Будем считать, что в ИС осуществляются логические алгоритмические вычисления, реализующие механизм принятия решений, включающий аппарат логического вывода, происходит формирование, расширение, преобра-

зование подсистемы знаний ИС. Уровень, на котором реализуются перечисленные процедуры, мы будем идентифицировать с понятием «сознание».

Информационное функционирование ИС, однако, не исчерпывается процессами, реализуемыми на данном уровне. Предполагается, что ИС способна также реализовывать алогические функции, базирующиеся, в частности, на аппарате нелинейной динамики[15]. Уровень, на котором функционирует данный аппарат, будем связывать с понятием «подсознание» («бессознательное»)[16].

В качестве модели, описывающей функционирование ИС на «сознательном» уровне, будем использовать модель-универсум информации ИЭП САМ ОР[17]. Абстрактной экспликацией модели-универсума И. в контексте представления и моделирования знаний является *k-гиперпространство семиотико-хроматических (СХ-) гипертопографов* ($\eta\tau$*-графов*) $\Gamma\mathfrak{S}$ [18]. Используемая экспликация модели-универсума обеспечивает моделирование и сенсориума, и подсистем знаний и коммуникации, и пространство целей, и объектов внешней среды, их свойств и отношений. Поскольку подсистема знаний относится к динамическим системам, в качестве динамических моделей представления знаний в зависимости от постановки задач используются конечные *метаалгебраической системы*, *метаалгебры* и *метаавтоматы,* или *семиотико-хроматические гипертопосети*[19].

Рассмотрим подробнее модель *k-гиперпространства* $\Gamma\mathfrak{S}$. *К-гиперпространство СХ-*$\eta\tau$*-графов* $\Gamma\mathfrak{S}$ есть допустимое множество семиотико-хроматических $\eta\tau$*-графов* $\{HTG_V^k x\}$ уровня топологизации k порождающие объекты представителей $HTG_V^k x$: $(V_\tau^k x, E_{\eta\tau}^k x, P_\tau^k)$, $HTG_V^k x \in \{HTG_V^k x\}$, $V_\tau^k x \subseteq V_\tau^k \times P^{V_\tau^k}$, $E_{\eta\tau}^k x \subseteq \subseteq E_{\eta\tau}^k \times P^{E_{\eta\tau}^k}$, $P_\tau^k \equiv P^{V_\tau^k} \cup P^{E_{\eta\tau}^k}$, которого, а именно V_τ^k и $E_{\eta\tau}^k$, есть элементы соответственно булеанов $\mathfrak{B}_k^V$ и $\mathfrak{B}_{k+1}^V$ k-го и $k+1$-го уровней топологизации множества-носителя V. Гипертопограф (монохромный) уровня топологизации k $HTG_V^k : (V_\tau^k, E_{\eta\tau}^k)$, $HTG_V^k \in \{HTG_V^k\}$ есть *опорный* $\eta\tau$*-граф* k-го уровня топологизации *СХ-*$\eta\tau$-графа $HTG_V^k x$.

Синтез модели *монохромного* k-гиперпространства $\Gamma\mathfrak{S}^m$ осуществлен путем последовательной топологизации множества-носителя гипертопографа V в булеан $\mathfrak{B}_k^V$ уровня топологизации k ($V \equiv \mathfrak{B}_0^V \subset \mathfrak{B}_1^V \subset \mathfrak{B}_2^V \subset ... \subset \mathfrak{B}_k^V$)[20]. Булеан $\mathfrak{B}_k^V$ уровня топологизации k есть результат последовательной k-топологизации *множества-носителя* $\eta\tau$-графа $V \equiv \mathfrak{B}_0^V$, $|V| = n$, когда на очередном этапе топологизации $i+1$ в качестве исходных неделимых и различимых элементов множества, порождающих булеан $\mathfrak{B}_{i+1}^V$, выступают непустые элементы булеана $\mathfrak{B}_i^V$. Показано, что для любого конечного уровня топологизации $k+1$ $(k \geq 0)$ совокупная мощность булеана $\mathfrak{B}_{k+1}^V$ (с элементом $\varnothing$) есть величина $|\mathfrak{B}_{k+1}^V| = 2^{2^{\cdot^{\cdot^{\cdot^{2^{|V|}-1}}}}-1}\}$ (k экземпляров 2 в показателе). Вследствие выполнения условия $HTG_V^k \subseteq \mathfrak{B}_{k+1}^V$ для $HTG_V^k \in \{HTG_V^k\}$ (произвольный гипертопограф HTG_V^k с носителем V уровня топологизации k есть некоторое *подмножество* булеана $\mathfrak{B}_{k+1}^V$ $k+1$ уровня топологизации множества-носителя – *элемент* («точка») булеана $k+2$ порядка $\mathfrak{B}_{k+2}^V$[21]) на $\Gamma\mathfrak{S}^m$ определено биективное соответствие

$$\{HTG_V^k\} \leftrightarrow \mathfrak{B}_{k+1}^V \qquad (1)$$

В качестве базовой модели «бессознательного» («подсознание») используем p-адическую модель мышления[22].

Рассмотрим множество 2-адических целых чисел $\mathbb{Z}_2$. Пусть $x = (\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, ...)$, $y = (\beta_0, \beta_1, \beta_2, ..., \beta_n, ...) \in \mathbb{Z}_2$, α_n, $\beta_n \in \{0,1\}$. Фиксируем действительное число $0 < q < 1$. Положим $\rho_2(x,y) = q^t$, если $\alpha_j = \beta_j$, $j = 0,1,...,t-1$, и $\alpha_t \neq \beta_t$. Эта функция является *ультраметрикой*[23]. Для того чтобы найти расстояние $\rho_2(x,y)$ между двумя последовательностями цифр x и y, мы должны найти первую позицию t такую, что последовательности

имеют различные цифры на этой позиции. Выбор константы q не играет никакой роли. Геометрии (топологии), соответствующие различным $0 < q < 1$, эквивалентны. В нашем случае $q = 1/2$. Таким образом $\rho_2(x, y) = 1/2^t$. Тогда $(\mathbb{Z}_2, \rho)$ – ультраметрическое пространство[24].

На множестве 2-адических чисел $\mathbb{Z}_2$ можно ввести алгебраические операции, а именно сложение, вычитание, умножение и деление. Эти операции являются естественными продолжениями стандартных операций на множестве $\mathbb{N}$.

Рассмотрим отображение: $f : \mathbb{Z}_2 \to \mathbb{Z}_2$, $x \to f(x)$. Итерации вида $x_n = f^n(x_0)$, $x_0, x_n \in \mathbb{Z}_2$, где $f^n(x) = f \circ ... \circ f(x) = f(...f(f(x))...)$ есть n последовательных применений отображения f. Зафиксировав функции вида $f : \mathbb{Z}_2 \to \mathbb{Z}_2$, мы моделируем процесс мышления на уровне «подсознания» посредством динамической системы $x_n = f(x_{n-1})$ на пространстве $\mathbb{Z}_2$. Начиная с x_0, мы получаем цепь $x_0, x_1, ..., x_n, ...$. Это и есть модель процесса «подсознательного» мышления. В общей постановке нас интересует непрерывное отображение $f : \mathbb{Z}_2 \to \mathbb{Z}_2$. Таким образом, в настоящей работе в качестве обобщенной модели процесса мышления на уровне «подсознания», мы определяем 2-адическую модель динамической системы на ультраметрическом неархимедовом пространстве[25].

Стоит отметить, что в 2-адической модели мышления важную роль играет то, на какой позиции стоят элементы $\alpha_j \in \{0,1\}$ в векторе $x \in \mathbb{Z}_2$. Это отражает фактор субъективности ИС, когда каждый элемент α_j характеризуется собственным приоритетом («значимостью»): на первом месте в векторе стоит наиболее «важный» элемент, затем менее «важный» и т. д.

Заметим, что множество всех векторов, у которых, начиная с какого-то места, во всех позициях стоят нули (т. е. векторы с конечным числом единиц) можно отождествлять с множеством $\mathbb{N}$ (плотным подмножеством в $\mathbb{Z}_2$). В качестве упрощенной модели

процесса мышления на уровне «подсознания» можно использовать динамическую систему на множестве натуральных чисел[26].

Представленные модели опираются на различные феноменологии моделирования процессов мышления. В рамках актуальной проблемы конструктивного синтеза обобщенной модели автономной самообучаемой ИС произвольного генезиса рассмотрим задачу объединения вышерассмотренных моделей в гибридную модель более высокого порядка в отношении изложенных. Основное внимание сосредоточим на прагматическом аспекте синтеза модели информационного запроса из области «сознания» в область «подсознания», т. е. формирования начального (стартового) состояния модели динамической системы «подсознания».

3. МОРФИЗМЫ МОДЕЛЕЙ МЫШЛЕНИЯ УРОВНЕЙ «СОЗНАНИЕ–ПОДСОЗНАНИЕ»

Ограничимся случаем, когда подсистема знаний ИС функционирует на k-гиперпространстве монохромных гипертопографов $\Gamma\mathfrak{s}^m$ [27]. Зафиксируем уровень топологизации k, характеризующий степень детализации объектов $\Gamma\mathfrak{s}$. K-гиперпространство $\Gamma\mathfrak{s}^m$ есть множество всех *потенциально* возможных монохромных гипертопографов. Для конкретной ИС ξ в этом пространстве актуализированы лишь определенные точки, представляющие собой знания, присущие непосредственно подсистеме знаний ИС ξ.

Если $V=(x_1,\ldots,x_n)$, $|V|=n$ – произвольное нумерованное конечное множество, $\mathfrak{B}^V$ – булеан множества V, то можно синтезировать конечномерное векторное булево пространство $[GF(2)]^{|V|}$, используя отображение ϕ_1: каждому из элементов $\mathfrak{b}^{x_l}\in\mathfrak{B}^V$ $(\mathfrak{b}^{x_l}\subseteq V)$, $l=\overline{1,2^n}$, однозначно характеризуемому как подмножеству V упорядоченным набором натуральных индексов $(i_1,\ldots,i_k)$, $i_j\in\overline{1,n}$, $j=\overline{1,n}$, $i_r\neq i_s$ для $\forall\, r\neq s$ и $i_r<i_s$ при $r<s$, поставлен во взаимно однозначное соответствие булев вектор (точка $[GF(2)]^{|V|}$) $\vec{\beta}_{\mathfrak{b}^{x_l}}=(\underset{1}{0}\ldots\overset{i_1\ldots i_k}{\underset{\ldots}{1}\ldots 1}\ldots\underset{n}{0})$ длины $n=|V|$, упорядоченный в порядке нумерации вектора $(i_1,\ldots,i_k)$, единицы в котором распо-

лагаются на местах соответствующих значениям индексов $i_1,\ldots,i_k$, а нули – на всех оставшихся местах (*индикатор* подмножеств дискретных топологий с нумерованным носителем V)[28].

Фактически каждой точке пространства монохромных гипертопографов в соответствие поставлен булев вектор (точка) $[GF(2)]^{|V|}$. Выделенный уровень топологизации k фактически характеризует степень детализации модели: чем больше k, тем более детализированы объекты на высших уровнях топологизации (для «*неатомарных*» элементов в *ZFU*, т. е. «разделимых» объектов уровня топологизации k)[29]. В результате, если V – множество-носитель $|V|=n$, то на уровне топологизации $k=1$ имеем 2^n векторов длины n. На уровне топологизации $k=2$ -2^{2^n-1} векторов-индикаторов длины 2^n и т. д.

Уточним структуру взаимно однозначного соответствия[30]

$$\mathfrak{B}_{i+1}^V \leftrightarrow [GF(2)]^{|\mathfrak{B}_i^V|} \qquad (2)$$

По определению $\mathfrak{B}_0^V \equiv (x_1, ..., x_n) \equiv V$, $|V|=n$. В терминологии векторных пространств элементы x_i, $i=\overline{1,n}$ есть точечные скаляры ($|x_i|=1$). Соответственно $\mathfrak{B}_0^V \equiv V$ соответствует вырожденный случай булева пространства $[GF(2)]$ мощности 1, а именно булев вектор $\vec{\mathfrak{b}}_0^V = (1, ...,1)$ размерности n. Булеан $\mathfrak{B}_1^V$ уровня топологизации 1 (классический булеан $\mathfrak{B}^V$ конечного множества V) есть множество подмножеств $\mathfrak{B}_0^V$ вида (x_1), ..., (x_n), (x_1,x_2), ..., $(x_1, ..., x_n)$, где элементы $x_i, i=\overline{1,n}$ есть неделимые различимые объекты $\mathfrak{B}_0^V$, и $\varnothing$ – как элемент $\mathfrak{B}_1^V$. Введение отображения ϕ: $\mathfrak{b}_1^V \to \vec{\mathfrak{b}}_1^V$, где $\mathfrak{b}_1^V \in \mathfrak{B}_1^V$ и $\vec{\mathfrak{b}}_1^V \in [GF(2)]^{|\mathfrak{B}_0^V|}$, определяющего взаимно однозначное соответствие $\mathfrak{B}_1^V \leftrightarrow [GF(2)]^{|\mathfrak{B}_0^V|}$, позволяет иденти-

фицировать элементы $\mathfrak{B}_1^V$ булевыми векторами размерности $|\mathfrak{B}_0^V|$. Индуктивное продолжение процесса топологизации V с последующей алгебраизацией модели приводит к следующим утверждениям[31].

Утверждение 1. Биективное соответствие $\mathfrak{B}_{i+1}^V \leftrightarrow$ $\leftrightarrow [GF(2)]^{|\mathfrak{B}_i^V|}$, порождаемое для произвольного конечного уровня топологизации i отображением $\phi : \mathfrak{b}_{i+1}^V \to \vec{\mathfrak{b}}_{i+1}^V$, где $\vec{\mathfrak{b}}_{i+1}^V$ – булев вектор размерности $|\mathfrak{B}_i^V|$, редуцирует на $\mathfrak{B}_{i+1}^V$ и $[GF(2)]^{|\mathfrak{B}_i^V|}$ изоморфизм универсальных алгебр $\mathfrak{A}_{\mathfrak{B}_{i+1}^V} =$ $= < \mathfrak{B}_{i+1}^V, (\cup, \cap) >$ и $\mathfrak{A}_{[GF(2)]^{\mathfrak{B}_i^V|}} = < [GF(2)]^{|\mathfrak{B}_i^V|}, (\vee, \wedge) > \triangleleft$

Обобщая вышеизложенные соображения в отношении рассматриваемых моделей подпроцессов мышления, сформулируем следующее утверждение.

Утверждение 2. Биективные соответствия (1) – (2): $\{HTG_V^k\}$ $\leftrightarrow$ $\mathfrak{B}_{k+1}^V$ $\leftrightarrow$ $[GF(2)]^{|\mathfrak{B}_k^V|}$ могут быть продолжены на $\mathbb{N}$ при $k \to \infty \triangleleft$

Доказательство.

Первая пара соответствий действительна согласно процедурам конструктивного синтеза $\{HTG_V^k\}$, $\mathfrak{B}_{k+1}^V$ и $[GF(2)]^{|\mathfrak{B}_k^V|}$.

Для любого конечного уровня топологизации $k+1$ ($k \geq 0$) совокупная мощность булеана $\mathfrak{B}_{k+1}^V$ (с элементом $\varnothing$) есть величина $|\mathfrak{B}_{k+1}^V| = 2^{2^{\cdot^{\cdot^{\cdot^{2^{|V|}-1}}}}-1}\}$ (k экземпляров 2 в показателе). Устремив

$k \to \infty$, получим, что $|\mathfrak{B}_{k+1}^V| \to \infty$. $\mathbb{N}$ – множество натуральных чисел – можно отождествлять со счетным множеством последовательностей 0 и 1 бесконечной длины (с конечным числом единиц), т. е. $[GF(2)]^{|\mathfrak{B}_k^V|} \leftrightarrow \mathbb{N}$ при $k \to \infty$. Соответственно,

$$\{HTG_V^k\} \leftrightarrow \mathfrak{B}_{k+1}^V \leftrightarrow [GF(2)]^{|\mathfrak{B}_k^V|} \leftrightarrow \mathbb{N} \qquad (3)$$

при $k \to \infty$. Что и требовалось доказать $\triangleleft\triangleleft$

Таким образом, переходя на все более и более высокий уровень топологизации, количество векторов растет с гиперэкспоненциальной сложностью. Если не менять уровень атомизации, то и длины векторов также растут гиперэкспоненциально. Учитывая, что все векторы уровня топологизации k согласуются с векторами уровня $k+1$ (добавлением определенного количества нулей в конец вектора – до необходимой длины), можно последовательно переходить на любой уровень топологизации больший k.

Построенное биективное отображение синтезирует информационный запрос из области «сознания» в область «подсознания», т. е. формирует начальное («стартовое») состояние модели динамической системы «подсознания». Модель «подсознания» начинает свою работу с этого состояния. В простейшем случае ее функционирование может рассматриваться как динамика на $\mathbb{N}$. В более сложном варианте можно рассматривать сформированное стартовое состояние как ссылку на некоторое множество $A \in \mathbb{Z}_2$, близких к нему с точки зрения метрики ρ_2 2-адических чисел. В этом случае результатом работы «подсознания» будет 2-адический образ – $B = f(A) = \{y = f(x) : x \in A\}$. Образ B, в свою очередь, представляет собой множество близких 2-адических чисел (динамика «ассоциаций»[32]). Чтобы интерпретировать полученный результат, необходимо «обрезать» множество B до одного представителя. Сделать это можно либо выделив в нем общий корень, т. е. сопоставить множеству B некоторое натуральное число, близкое всем элементам множества B, либо выбрать из B один представитель и «обрезать» его до натурального числа. Сделать это всегда возможно со сколь угодной точностью в силу плотности

множества $\mathbb{N}$ в $\mathbb{Z}_2$. Таким образом, в результате работы динамической системы «подсознания» мы получаем в некотором смысле «размытое», а не точное решение вследствие «отсечения» континуального множества «хвостов» при переходе от $\mathbb{Z}_2$ к $\mathbb{N}$.

Подчеркивая важность порядка элементов $\alpha_j \in \{0,1\}$ в векторе $x \in \mathbb{Z}_2$ в 2-адической модели мышления (все α_j имеют собственный приоритет), отметим, что реализуя биективное отображение (соответствие), мы фактически отказываемся от вышеупомянутой «субъективности» модели ИС. Однако для большинства приложений «разнозначимость» скаляров в векторе может оказаться весьма существенной.

Поставим в соответствие каждому булевому вектору $\vec{\alpha}$ (точке $[GF(2)]^{|\mathfrak{B}_k^V|}$) вектор $\vec{K}_\alpha = (k_1,...,k_v,...,k_q,...,k_n)$, где $k_q \in (0,1]$ и $k_q \neq k_v$. Таким образом, если $\vec{\alpha} = (\alpha_1,...,\alpha_q,...,\alpha_n)$, то k_q есть вес q-го элемента вектора α. Значения k_q выбираются в соответствии с «важностью» («значимостью»)[33] q-го скаляра вектора $\vec{\alpha}$. В результате получаем для каждого вектора $\vec{\alpha}$ нормированную шкалу весов его скаляров. Переставим местами скаляры вектора $\vec{K}_\alpha$ по убыванию значений элементов k_q, получим вектор $\vec{K}_{\alpha_{упор}}$ (*упорядоченный*), где на первом месте стоит наибольший k_q, затем k_v, так что $k_v < k_q$ и т. д. Преобразуем вектор $\vec{\alpha}$ в вектор $\vec{\alpha}_{упор}$ путем перестановки скаляров α_q в соответствии с местом соответствующего веса k_q. Обозначим такое преобразование вектора $\vec{\alpha}$ в вектор $\vec{\alpha}_{упор}$ через φ. Фактически частное преобразование $\varphi(\vec{\alpha}) \equiv \vec{\alpha}_{упор}$ порождает отображение общего вида $\Phi\ [GF(2)]^{|\mathfrak{B}_k^V|} \to [GF(2)]^{|\mathfrak{B}_k^V|}$.

Введем на множестве векторов $[GF(2)]^n$ бинарное отношение θ: два вектора $\vec{\alpha}, \vec{\beta} \in [GF(2)]^n$ находятся в отношении θ ($\vec{\alpha} \overset{\theta}{\sim} \vec{\beta}$), если в результате преобразования φ, примененного к каждому из них, получившиеся вектора $\vec{\alpha}_{упор}, \vec{\beta}_{упор}$ равны, т. е. $\rho_h(\vec{\alpha}_{упор},$

$\vec{\beta}_{упор}) = 0$, где ρ_h – метрика Хэмминга. В отношении θ справедливо следующее утверждение.

Утверждение 3.

A. Отношение θ есть отношение эквивалентности на $[GF(2)]^n$.

B. Отношение θ разбивает множество векторов $[GF(2)]^n$ на непересекающиеся классы эквивалентности. Класс эквивалентности содержит все векторы $\vec{\alpha}, \vec{\beta} \in [GF(2)]^n$, для которых $\rho_h(\vec{\alpha}_{упор}, \vec{\beta}_{упор}) = 0 \triangleleft$.

Доказательство.

A. 1. Рефлексивность. Очевидно в виду однозначности построение вектора $\vec{\alpha}_{упор}$ $\forall \vec{\alpha} \in [GF(2)]^n$. 2. Симметричность. $\forall \vec{\alpha}, \vec{\beta} \in [GF(2)]^n$, если $\rho_h(\vec{\alpha}_{упор}, \vec{\beta}_{упор}) = 0$, то и $\rho_h(\vec{\beta}_{упор}, \vec{\alpha}_{упор}) = 0$. 3. Транзитивность. $\forall \vec{\alpha}, \vec{\beta}, \vec{\gamma} \in [GF(2)]^n$, если $\rho_h(\vec{\alpha}_{упор}, \vec{\beta}_{упор}) = 0$ и $\rho_h(\vec{\beta}_{упор}, \vec{\gamma}_{упор}) = 0$, то $\vec{\alpha}_{упор} = \vec{\beta}_{упор}$ и $\vec{\beta}_{упор} = \vec{\gamma}_{упор}$, следовательно $\vec{\alpha}_{упор} = \vec{\gamma}_{упор}$, $\rho_h(\vec{\alpha}_{упор}, \vec{\gamma}_{упор}) = 0$.

B. Последующее доказательство очевидно и вытекает из общей теории отношений и процедур построения фактор-множеств (разбиения множеств по отношению эквивалентности) $\triangleleft\triangleleft$.

Применяя преобразование φ ко всем точкам $[GF(2)]^{|\mathfrak{B}_k^V|}$, мы можем провести разбиение $[GF(2)]^{|\mathfrak{B}_k^V|}$ на вышеупомянутые классы эквивалентности и определить все $\vec{\alpha}_{упор}$ (образующие) однозначно их характеризующие.

Преобразование φ фактически реализует сюръективное отображение $[GF(2)]^{|\mathfrak{B}_k^V|} \to \overline{[GF(2)]^{|\mathfrak{B}_k^V|}}$, $\overline{[GF(2)]^{|\mathfrak{B}_k^V|}} \subseteq [GF(2)]^{|\mathfrak{B}_k^V|}$. Таким образом, цепочка соответствий (3) расширяется до следующей:

$$\{HTG_V^k\} \leftrightarrow \mathfrak{B}_{k+1}^V \leftrightarrow [GF(2)]^{|\mathfrak{B}_k^V|} \to \overline{[GF(2)]^{|\mathfrak{B}_k^V|}} \leftrightarrow \mathbb{N} \qquad (4)$$

при $k \to \infty$.

В результате работы модели динамической системы «подсознания» мы получаем точку $[GF(2)]^{|\mathfrak{B}_k^V|}$, которую в настоящих условиях невозможно однозначным образом идентифицировать конкретным актуальным $\Gamma\mathfrak{s}$-объектом. Однако согласно утверждению 3, мы имеем возможность идентифицировать некоторый «размытый» («*диффузный*»)[34] результат работы «подсознания», соотнеся его с некоторым *классом* гипертопографов. Такая «размытость» вполне соответствует эмпирическим наблюдениям в области психологии и может быть охарактеризована как интуитивно-образное мышление.

ЗАКЛЮЧЕНИЕ

Предложенные процедуры построения соответствий и отображений используемых моделей позволяют реализовать механизм формирования информационного запроса из подпроцесса уровня «сознания» в подпроцесс уровень «подсознания» с сохранением прагматической разнозначимости структуры запроса. Обратное отображение результата функционирования модели «подсознания» на уровень «сознания» носит «диффузный» характер. Решение вопроса о возможности однозначной интерпретации информационного запроса на уровне «сознания» требует продолжения исследований в выбранном направлении.

Наряду с рассмотренным механизмом взаимодействия моделей подпроцессов мышления можно предложить и подход, основанный на существенном изменении феноменологии синтеза гипертопографов. А именно подход, основанный на отказе от принципа построения множества-носителя в рамках аксиоматической системы *ZFU* (с «праэлементами»). В данной постановке предполагается переход к синтезу так называемых *континуальных* гипертопографов $\{HTG^k_{card\,\mathbb{R}}\}$, в качестве множества-носителя которых определено множество мощности континуума. Последнее, близкое к понятию гипермножества[35], синтезируется с использованием принципа «бесконечной» *делимости* «целого» на «части». В этом случае появляется возможность исследования «естественного» биективного соответствия $\{HTG^k_{card\,\mathbb{R}}\} \leftrightarrow \mathbb{Z}_2$.

Реализация 2-адической модели мышления (уровня «подсознания») может быть спроецирована на аппарат нейронных сетей (в рамках естественных ограничений на конечность нейронных структур)[36]. Каждый нейрон, в простейшей дискретной интерпретации, имеет две степени возбуждения: 1 – возбуждение, 0 – отсутствие возбуждения. Когнитивная информация представляется цепью нейронов. Каждая цепь имеет иерархическую структуру, которая основывается на способности нейрона возбудить последовательность нейронов в цепи (первый нейрон наиболее «важен», так как способен возбудить все последующие нейроны в цепи, второй менее «важен», чем первый, так как не может возбудить предшествующий нейрон, и т. д.).

В перечень последующих исследований предполагается включить и задачи расширения механизма синтезированных отображений (соответствий) на случай полихромных гипертопографов, построения обратного отображения для случая с приоритетами α_j, изучения условий применимости и эффективности реализации различных функций f на $\mathbb{Z}_2$, алгоритмизации разработанного аппарата взаимодействия с целью синтеза имитационно-компьютерных моделей подпроцессов мышления.

АББРЕВИАТУРЫ

АИКИ – атрибутивно-ингредиентная концепция информации
ЕЯ – естественный язык
И. – информация
ИС – интеллектуальная система
ИЭП – информационно-эволюционный подход
КС –кибернетическая система
МС –материальная система
ОР – объективная реальность
САМ – системный анализ и моделирование

Примечания

[1] См.: *Баранович А.Е.* О систематизации аксиоматического аппарата предметной области «Искусственный интеллект» / Интеллектуальные системы. Т. 14, Вып. 1–4. М., 2010. С. 5 –34.

[2] См.: Центр системного анализа и моделирования мышления [Электрон. ресурс]. [М., 2011]. URL: www.samtcenter.ru

[3] См.: *Блумфилд Л.* Язык / Пер. с англ. Е.С. Кубряковой и В.П. Мурат. Под ред. и с предисл. М.М. Гухман. М.: Прогресс, 1968. 608 с.

[4] Обычно *модель* – упрощенный, искусственно синтезированный объект, используемый для представления более сложного реального.

[5] См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу: Учеб. пособие. М.: РГГУ, 2011. 268 с.

[6] См.: *Баранович А.Е.* О систематизации аксиоматического аппарата предметной области «Искусственный интеллект».
См.: *Баранович А.Е.* Информационно-эволюционный подход в теории интеллектуальных систем / Матер. X Междунар. конф. «Интеллект. системы и компьют. науки». М.: МГУ, 2011 (в печ.).

[7] См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу.

[8] В настоящей реализации Вселенной.

[9] Управления с обратными связями.

[10] См.: *Baranovich A.E.* Concept of operated evolution of a natural language: problem statement / Proc. of the 12th Intern. Conf. “Speech and Computer” SPECOM’2007. Vol. 2. Moscow, Moscow State Linguistic Univ., 2007. P. 823–832.

[11] См.: *Баранович А.Е.* Введение в информациологию и ее специальные приложения: дидактические материалы к специальному курсу.
См.: *Баранович А.Е.* Введение в предметно-ориентированные анализ, синтез и оптимизацию элементов архитектур потоковых систем обработки данных. 2-е изд., испр. и дополн. М: МО РФ, 2001. 277 с.

[12] Философии.

[13] В упрощенной интерпретации – *атрибут*.

[14] Как процесса.

[15] См.: *Кадомцев Б.Б.* Динамика и информация. М.: Наука, 1998. 394 с.;
См.: *Капица С.П., Курдюмов С.П., Малинецкий Г.Г.* Синергетика и прогнозы будущего. М.: Наука, 1997. 285 с.

[16] См.: *Франц М.-Л.* Прорицание и синхрония: психология значимого случая / Пер. с англ. З. Кривулиной; Под общ. ред. В. Зеленского. СПб.: Азбука-классика», 2009. 224 с.

[17] См.: *Баранович А.Е.* Структурное метамоделирование телеологических информационных процессов в интеллектуальных системах. М.: МО РФ, 2002. 316 с.

[18] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: МО РФ, 2003. 404 с.

[19] См.: *Баранович А.Е.* Семиотико-хроматические гипертопосети: унифицированная модель представления знаний / Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): Матер. Междунар. научн.-техн. конф. // Редкол.: В.В. Голенков (отв. ред.) [и др.].Минск: БГУИР, 2011. С. 71–86.

[20] $\equiv V_{\aleph_0}$ – искусственный прием для граничного случая.

[21] См.: *Баранович А.Е.* Многоосновные СХ-гипертопографы – однообъектная парадигма // Тр. III Междунар. конгресса по интеллект. системам и информ. технол. / XI Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'11). М.: Физматлит, 2011. Т. 1. С. 377–385.

[22] См.: *Хренников А.Ю.* Моделирование процессов мышления в p-адических системах координат. М.: Физматлит, 2004. 295 с.

[23] См.: *Коблиц Н.* p-адические числа, p-адический анализ и дзета-функции. М.: Мир, 1981. 192 с.

[24] См.: *Хренников А.Ю.* Неархимедов анализ и его приложения. М.: Физматлит, 2003. 217 с.

[25] См.: *Хренников А.Ю.* Моделирование процессов мышления в p-адических системах координат.

[26] См.: Там же.

[27] Последующая хроматизация $\Gamma\aleph$ лишь мультипликтивно увеличивает размерность используемой модели, не оказывая принципиального влияния на феноменологию её использования.

[28] См.: *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, Главн. ред. физ.-мат. лит., 1982. 384 с.

[29] См.: *Баранович А.Е.* К вопросу идентификации тождественных объектов в модели k-гиперпространства СХ-гипертопографов / Тр. I Междунар. конгресса по интеллект. системам и информ. технол. // IX Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS'09). М.: Физматлит, 2009. Т. 1. С. 481–490.

[30] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект.

[31] См.: Там же (утверждение 4.1.9).

[32] См.: *Хренников А.Ю.* Моделирование процессов мышления в *p*-адических системах координат.

[33] См.: *Баранович А.Е.* Развитие модели *k*-гиперпространства СХ-гипертопографов на случай «разнозначимости» их элементов / Тр. II Междунар. конгресс по интеллект. системам и информ. технол. // X Междунар. научн.-техн. конф. «Интеллект. Системы» (AIS'10). Т. 2 М.: Физматлит, 2010. С. 3–10.

[34] Часто используемые в ряде предметных областей термины «нечеткие» модели, и в частности «нечеткие множества», не используются в настоящем материале вследствие: 1) фактической принадлежности упомянутых моделей классу детерминировано-четких, 2) существенно различной феноменологической интерпретации нами понятий «нечеткость» и «диффузность» («размытость»).

[35] См.: *Barwise J., Moss L.* Hypersets. // Mathematical Intelligencer. Vol. 13. No 4. 1991. P. 31–41; См.: *Barwise J., Moss L.* Vicious circles and the mathematics of non-well-founded, Phenomena. Stanford: CSLI Public., 1996. P. 390.

[36] См.: *Хренников А.Ю.* Моделирование процессов мышления в *p*-адических системах координат.

С.М. Иглицкая

ОБ ОДНОМ ПОДХОДЕ К МОДЕЛИРОВАНИЮ СЕМАНТИКИ ПОЛИФОНИЧЕСКОГО МУЗЫКАЛЬНОГО ТЕКСТА

Статья посвящена вопросам исследования информационной составляющей музыкального текста. Рассматривается возможность использования универсальной модели состояний сложных динамических систем для моделирования семантики многоголосного музыкального текста. Излагается ряд концептуальных подходов к построению моделей музыкальных текстов различных стилей.

Ключевые слова: текст музыкальный, семантика текста, полифония строгого стиля, k-гиперпространство СХ-гипертопографов, СХ-гипертопосети.

До настоящего времени информационная составляющая музыкального текста (МТ) исследована весьма поверхностно, к фактически неизученной области относятся вопросы семантики музыкальных произведений. Анализ доступных источников показывает, что большая часть работ в данной сфере имеет чисто гуманитарную направленность. Ряд актуальных вопросов поднимается в трудах М.Ш. Бонфельда[1], М.Г. Арановского[2] и С.Ю. Барановой[3], однако проблемы семантики рассмотрены в них исключительно в культурологическом аспекте. Среди редких удачных попыток объединения естественно-научного и искусствоведческого направлений можно назвать лишь уникальные работы Р.Х. Зарипова[4]. Подобные обстоятельства обусловлены отсутствием в классическом музыковедении как отрасли гуманитарного знания математических методов анализа МТ, с одной стороны, и редким обращением к нему как к объекту исследования в работах естественно-научной направленности, с другой стороны.

Ориентация на последовательное изучение модели семантики в применении к МТ позволяет обозначить ряд прагматических задач, связанных с характеризацией естественно-научного базиса МТ.

• Идентификация МТ. Установление авторства анонимных музыкальных произведений, определение стилистической принадлежности фрагмента МТ, распознавание по нотной записи вида оптимального для исполнения музыкального инструмента.

• Изучение характеристик канала музыкальной коммуникации. Исследование канала связи, использующего МТ, его пропускной способности, возможностей и методов передачи по нему различных видов информации, не исключая секретной[5].

• Анализ особенностей семантической музыкальной коммуникации коллектива антропоморфных интеллектуальных систем (АИС).

• Исследование прагматического потенциала (ПП) музыкальной информации.

Понятие ПП для музыкальной информации вводится по аналогии с таковым для вербальной информации (ВИ), определенным следующим образом[6]: «ПП ВИ есть неотъемлемое имманентное свойство ВИ, отражающее частные (лингвистические) особенности прагматических отношений и характеризующее допустимые возможности языка по идентификации общего многообразия (разнообразия, по Л. Бриллюэну–У. Эшби) объективной реальности в процессе семантической коммуникации АИС <...> Основной целью введения понятия ПП является его использование для качественного, а в последующем и количественного анализа синтеза И. с точки зрения ее неоднозначной (многозначной) интерпретации воспринимающим субъектом (объектом). <...> В случае текстуальной (“документальной”) коммуникации, мы имеем дело с информацией, отчужденной в пространстве времени от ее источника, когда ПП ВИ социально объективизирован (интерсубъективизирован) и его атрибуты в прагматическом отношении определяются только синтактикой (формальными лингвистическими характеристиками) и семантикой информации (на коллективной подсистеме знаний социума и индивидуальной подсистеме знаний получателя информации), но уже отчуждены от подсистемы знаний реципиента».

На предшествующем этапе исследований[7] был получен результат оценки пропускной способности дискретного канала связи по К. Шеннону, использующего МТ так называемого строгого стиля, представленный моделью дискретных сообщений Дж. фон Неймана

нулевого и первого приближений. Однако данная модель относится к классу последовательных семиотических моделей («семантически тривиальных») и, с одной стороны, требует упрощения МТ до уровня модели конечного алфавита, а с другой стороны, не отражает разнообразия структурных связей в нем, а лишь отношения n последовательных символов (разрешенные и запрещенные n-граммы).

Для более глубокого анализа МТ необходима модель, способная отразить отношения любых элементов текста (структуралистическая). Поэтому в дальнейших исследованиях мы будем опираться на модель k-гиперпространства СХ-гипертопографов как универсальную абстрактную модель информационной составляющей состояний сложных динамических систем.

1. Используемые понятия и модели

Пусть задано некоторое множество V, $|V| = n$. Гипертопограф[8] с носителем $VHTG_V$ есть двойка вида $(V_\tau, E_{\eta\tau})$, где $V_\tau \equiv \{\nu_\tau\}$ – некоторое подмножество элементов булеана B^V с носителем V, $V_\tau \subseteq \mathrm{B}^V$, $|V_\tau| \equiv \mathrm{N} \le 2^n$, и $E_{\eta\tau} \equiv \{e^k_{\eta\tau}\}$ – заданное множество подмножеств $e^k_{\eta\tau}$ множества V_τ, $e^k_{\eta\tau} \subseteq V_\tau$, различной мощности $|e^k_{\eta\tau}| = k$, $1 \le k \le N$, $e^k_{\eta\tau} \in V^{(k)}_\tau$, $|E_{\eta\tau}| = m$, $E_{\eta\tau} \subseteq \mathrm{B}^{V\tau}$,$\mathrm{m} \le 2^N$, $\le 2^n$.

Гипертопограф NTG^k_V с носителем V уровня топологизации k определяется как подмножество булеана B^V_{k+1} уровня топологизации множества-носителя ($NTG^k_V \subseteq \mathrm{B}^V_{k+1}$), где элементы NTG^k_V входящие в булеан B^V_k и не входящие в булеан B^V_{k+1}, т. е. не принадлежащие множеству $\mathrm{B}^V_{k+1} \setminus \mathrm{B}^V_k$, образуют множество его *топовершин* $V^k_\tau (V^k_\tau \subseteq NTG^k_V \subseteq \mathrm{B}^V_k, V^k_\tau \not\subset \mathrm{B}^V_{k+1} \setminus \mathrm{B}^V_k)$, а множество $E_{\eta\tau} \equiv NTG^k_V \setminus V^k_\tau$ – множество *гипертопоребер* NTG^k_V.

Для гипертопографов вводятся понятия хроматизации (каждому элементу $HTG_V \cdot (V_\tau, E_{\eta\tau})$ ставится в соответствие некоторое подмножество цветов из заданного множества P) и семиотизации (конструктивного поименования -$\eta\tau$-графа и элементов порождающих его множеств).

Семиотико-хроматическое k-гиперпространство СХ-$\eta\tau$-графов ΓS есть допустимое множество семиотико-хроматических $\eta\tau$-графов $\{NTG^k_V x\}$ уровня топологизации k, порождающие объекты представителей $NTG^k_V x$:$(V^k_\tau x,\ E^k_{\eta\tau} x,\ P^k_\tau)$, $NTG^k_V x \in \{NTG^k_V x\}$,

$V^k_\tau x \subseteq V^k_\tau \times P^{V\tau}$, $E^k_{\eta\tau} x \subseteq E^k_{\eta\tau} \times P^{V\eta\tau}$, $P^{V\tau} \equiv P^{V\tau} \cup P^{E\tau}$ которого, а именно V^k_τ и $E^k_{\eta\tau}$, есть элементы соответственно булеанов B^V_k и B^V_{k+1} k-го и k +1-го уровней топологизации множества-носителя V.

В модели *СХ-гипертопосети*[9] модель k-гиперпространства СХ-гипертопографов используется в качестве допустимого множества изменяющихся статических состояний модели. Динамические процессы преобразования информации (механизмы их реализации) в сети моделируются *функциональными* («процедурными» в инженерной терминологии) *преобразователями* как *топовершинной*, так и *гипертопореберной* принадлежности (в моделях как «квантованного времени», так и времени по «наступлению события»).

Множество функциональных преобразователей информации (процедур) декларируется расширением обобщенного множества хроматических атрибутов (и их значений) СХ-$\eta\tau$-графа NTG^k_V: ($V^k_\tau x$, $E^k_{\eta\tau} x$, P^k_τ), $P^k_\tau \equiv \{{}_{D_c} P^k_\tau \cup {}_{\mathrm{P_r}} P^k_\tau\}$, *где декларативные знания* (*Dc*) образуют известное подмножество ${}_{D_c} P^k_\tau$, ${}_{D_c} P^k_\tau \equiv {}_{\mathrm{P_r}} P^{V^k_\tau} \cup P^{E^k_{\eta\tau}}$, а *процедурные* (*Pr*) – подмножество ${}_{\mathrm{P_r}} P^{V^k_\tau}$, $\equiv {}_{\mathrm{P_r}} P^{V^k_\tau} \cup P^{E^k_{\eta\tau}}$.

При изучении вопросов моделирования семантики МТ необходимо различать объективную семантику, присущую самой информации, и субъективную (прагматическую) семантику, зависящую от воспринимающего субъекта. По определению А.Е. Барановича[10], «*объективная семантика* информации характеризует информационные формы существования материальных систем объективной реальности и взаимосвязана с формой, структурой и организацией материальных систем. ... В свою очередь, семантика субъективная (прагматическая) интерпретируется как динамический информационный образ объективной семантики (информации материальной системы “внешнего мира”), инициализированный в подсистеме знаний воспринимающей интеллектуальной системы».

Таким образом, необходимо в первую очередь изучить модель объективной семантики, т. е. модель структуры.

Для представления МТ возможно использование в качестве базовой как статической модели СХ-гипертопографа, так и динамической модели СХ-гипертопосети. Приоритет в выборе того или иного подхода зависит от стилистических особенностей анализируемого (моделируемого) МТ: если обладающую развитой совокупностью структурных связей сонатную форму целесообразно представить в виде статической модели, то аморфный по форме

(т. е. характеризуемый слаборазвитыми связями между удаленными элементами), но обладающий строго детерминированными правилами соотношения соседних созвучий полифонический МТ строгого стиля представляется логичным исследовать с применением аппарата моделирования динамических систем.

2. Проекция нотации музыкального произведения на модель сх-гипертографа

Письменный МТ представляет собой совокупность символов, основными из которых (определяющими высотно-временные параметры звучания музыкального произведения) являются ноты и паузы (которые могут быть трактованы как «беззвучная» нота определенной длительности), дополнительные же знаки (штрихи, динамические указания, знаки музыкального синтаксиса – ферматы, фразировочные лиги) относятся к средствам музыкальной выразительности.

При выборе множества-носителя конструируемой модели естественно опираться только на основные символы, при этом будем исходить из того, что каждая нота обладает двумя базовыми характеристиками – высотой и длительностью. В работе с моделью Дж. фон Неймана в качестве символов формируемого алфавита мы брали все возможные сочетания длительностей и звуковысотных положений нот. При использовании модели СХ-гипертопографов логичным представляется один из этих параметров использовать как базовый, а другой отразить как хроматический атрибут вершины, при этом имя последней может включать информацию об обеих характеристиках (например: «до малой октавы, восьмая»).

На первый взгляд кажется более удобным представить множество-носитель набором всех возможных длительностей нот, так как это графически ясно различимые и однозначно интерпретируемые символы, тогда как высота ноты графически обозначается только ее положением на нотном стане и определяется ключом (т. е. одно и то же положение может означать разные звуки). Кроме того, существуют музыкальные инструменты без определенной высоты звука (бубен, барабан, треугольник), для которых ритмическая составляющая является единственной определяющей характеристикой.

С другой стороны, в произведениях определенных стилей ритмическая организация может быть весьма сложной и точное опре-

деление длительностей некоторых нот может оказаться невозможным (например, при отсутствии размера и указании *rubato*), в то время как высота звука является его абсолютной (физической) характеристикой, набор используемых высот ограничен пределами возможностей слухового восприятия и может быть представлен (по крайней мере, в европейской культуре) дискретной шкалой с шагом в полутон.

Таким образом, выбор одного из двух подходов будет зависеть от стилистических особенностей произведения.

Следующий фактор, который необходимо учитывать – это повторяемость элементов МТ, от нот и аккордов до продолжительных законченных построений.

Поэтому предлагается использовать модифицированную модель СХ-гипертопографа с расширенным множеством-носителем, характеризующим множественность различимых (посредством хроматических атрибутов) экземпляров односортных элементов[11] (дальнейшая топологизация реализуется согласно классической модели СХ-гипертопографа). В качестве элементов множества-носителя берутся все нотные знаки произведения, а различные уровни топологизации отражают иерархию связей между ними.

Вершины первого уровня топологизации представлены одноточечными элементами множества-носителя; все характеристики, относящиеся к отдельной ноте (тембр, громкость, артикуляция, а также координаты в произведении – принадлежность определенному голосу и место в такте), могут быть отражены в хроматических атрибутах вершины.

На следующем уровне топологизации возможно два типа отношений: вертикальное – объединение одновременно звучащих нот в аккорд; горизонтальное – объединение подряд идущих нот в музыкальную фразу. Здесь могут возникнуть некоторые сложности, связанные со спецификой МТ. Если для вербального текста при аналогичном подходе к формированию множества-носителя дальнейшая топологизация очевидна (буквы объединяются в слова, слова в предложения и так далее), то для МТ понятие «музыкальная фраза» весьма расплывчато, их строение во многом зависит от индивидуальных особенностей стиля конкретного произведения, кроме того, возможно пересечение соседних фраз, когда окончание одной является началом следующей. Тем не менее выделение некоторых структурных единиц в отдельно взятой мелодической линии всегда возможно[12], из этого следует потенциальная возможность алгоритмизации данной процедуры.

Дальнейшая топологизация предполагает объединение фраз отношениями, например, повтора, противопоставления, эха, секвенции, вариации и т. д.

На последнем уровне должны быть отражены отношения между частями музыкальной формы (например, экспозиция–реприза).

Данный подход к представлению музыкального произведения дает возможность более строгого определения в терминах конструируемой модели некоторых гуманитарных понятий, относящихся к области музыковедения, а также устоявшихся неформальных выражений из сферы исполнительской практики.

В частности, степень художественной ценности произведения во многом определяется количеством и структурой связей между его элементами, т. е. количеством и характеристиками гипертопоребер на всех уровнях топологизации. Способность создания произведений с развитой системой связей характеризует, с определенных позиций, меру таланта композитора, а способность выявлять эти связи – меру таланта исполнителя или музыковеда. Развитие данных способностей (в совокупности с техническими навыками) относится к основам обучения в музыкальном учебном заведении.

Выражение «исполнитель выстроил произведение по форме» может быть интерпретировано с использованием вышевведенного терминологического аппарата следующим образом: исполнительскими средствами (с использованием доступных выразительных возможностей музыкального инструмента) хорошо отражены отношения элементов булеана последнего уровня топологизации; а выражение «играть крупным помолом» означает отсутствие или искажение отношений на первых уровнях топологизации модели.

При дальнейшем развитии подобного похода возможна разработка объективного критерия оценки исполнения музыкального произведения, что является весьма актуальной задачей в настоящее время в связи с большим количеством музыкальных конкурсов, традиционно вызывающих огромное количество споров как в профессиональной, так и в любительской среде.

3. Моделирование музыкального текста строгого стиля аппаратом семиотико-хроматических гипертопосетей

Строгий стиль[13] (С.С.) – историческое и художественно-стилистическое понятие, относящееся к хоровой полифонической

музыке эпохи Ренессанса (XV–XVI вв.). Относительное стилистическое единство музыки эпохи С.С., простота мелодико-гармонических и ритмических норм позволяет изложить основы контрапункта в виде сравнительно небольшого числа точных правил и формул, что является исключительным свойством по отношению к другим музыкальным стилям, нормы которых большей частью весьма расплывчаты и практически не поддаются алгоритмическому описанию.

Данная особенность МТ С.С. определила его выбор в качестве основного объекта изучения как на предшествующем, так и на настоящем этапе исследований. Основным музыковедческим источником является учебник полифонии В.П. Фраенова[14], где приведено точное изложение формализованных правил С.С.

При моделировании МТ аппаратом семиотико-хроматических гипертопосетей логично в качестве статических состояний, представленных СХ-гипертопографами, рассматривать все вертикальные (одновременно звучащие) соединения (созвучия), априорно обладающие собственной сложной структурой отношений (особенно для полифонической музыки). При этом изменение любой ноты ведет к переходу в следующее состояние в модели времени «по наступлении события».

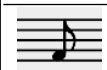
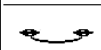
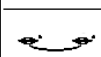
Поскольку в полифоническом МТ строго детерминирована принадлежность ноты определенному голосу (мелодической линии, предназначенной для одного исполнителя или группы исполнителей в унисон), определим множество-носитель как совокупность наборов всех возможных звуковысотных положений для всех голосов (при этом каждый элемент включает идентификатор, обозначающий его принадлежность определенному голосу). Для каждого голоса это число равно 14, так как вне зависимости от голоса и ключа диапазон для всех них ограничен одними и теми же рамками (рис. 1). Таким образом, мощность множества-носителя равна 14 n, где n – число голосов моделируемого МТ.

Рис. 1

В качестве вершин 1-го уровня топологизации выберем множество n одноэлементных подмножеств множества-носителя, соответствующих одновременно звучащим в n голосах нотам (есте-

Таблица

Длительность нот

Графический символ ноты	Длительность	Количество восьмых долей
	Восьмая нота	1
	Четвертная нота	2
	Половинная нота	4
	Половинная нота, слигованная с четвертной нотой	6
	Целая нота	8
	Половинная нота, слигованная с половинной нотой	
	Целая нота, слигованная с половинной нотой	12
	Бревис	16
	Целая нота, слигованная с целой нотой	
	Целая нота с точкой (11/2 целой), слигованная с половинной нотой	
	Целая нота с точкой, слигованная с половинной нотой	20
	Целая нота с точкой, слигованная с целой нотой с точкой	24

ственно, идентификаторы принадлежности голосам должны быть у всех различными).

Декларативные знания топовершинной принадлежности представим следующими хроматическими атрибутами:

– длительность ноты; выражается в количестве восьмых долей; всего возможно 9 вариантов значений (таблица);

– координаты ноты в произведении; номер такта (тактов, если залигованная через тактовую черту нота расположена в двух соседних тактах); расположение относительно метрических долей.

Множество гипертопоребер является в этом случае множеством всех созвучий (интервалов и аккордов), образуемых нотами, выбранными в качестве вершин, а хроматические атрибуты характеризуют вертикальные, а также горизонтальные (с учетом длительностей нот) отношения между ними.

Для дальнейшего построения модели необходимо учесть следующее: в многоголосном МТ С.С. каждый голос подчиняется правилам одноголосия, каждая пара и тройка голосов – соответственно, правилам двух- и трехголосия; контрапунктические же условия для четырех и более голосов не отличаются от таковых в трехголосии. Поэтому формирование на первом уровне топологизации подмножеств мощности более трех не представляется целесообразным; кроме того, не требуется рассмотрения уровней топологизации выше двух (на втором уровне могут быть отражены отношения «пара голосов – третий голос» в трехголосии).

Для описания процедурных знаний необходимо представление неклассифицированных и несколько бессистемно изложенных у В.П. Фраенова правил С.С. (с математической точки зрения; в рамках учебно-методических задач усвоения материала студентами музыкальных учебных заведений подобное изложение вполне оправданно) в виде алгоритмов, относящихся к текущему состоянию модели.

Заключение

В настоящей статье рассмотрен ряд аспектов моделирования семантики МТ. Одним из главных факторов, существенно затрудняющих иконический анализ МТ, является фактическое отсутствие средств автоматизации его обработки (помимо программ нотного набора, обладающих весьма ограниченными функциями по автоматизации работы с МТ), что делает практически невозможной работу с большими корпусами текстов и, как следствие, проверку рабочих моделей и гипотез на значительных объемах структурированной информации. Если в области вербальных текстов значительная часть ресурсов культурного наследия уже длительное время представлена в оцифрованном виде, то объем представленных в доступном для автоматической обработки формате нот составляет лишь ничтожно малую долю возможного.

Тем не менее определенные усилия в данном направлении предпринимаются; в частности, существует несколько интернет-

библиотек, где представлено определенное количество нотно-музыкальных ресурсов (например, в формате музыкального редактора LilyPond)[15].

Создание такого рода библиотек и широкое внедрение методов автоматизации обработки МТ могло бы создать условия для решения многих проблем, касающихся как математической и естественно-научной, так и искусствоведческой стороны изучения МТ. Одним из наиболее актуальных и востребованных практических приложений данного направления могло бы служить создание музыкальной поисковой системы, аналогичной существующим системам для вербального текста. Участие в подобных проектах входит в круг прагматических интересов автора.

Данная работа носит постановочный характер и предопределяет продолжение исследований в направлении дальнейшей детализации и строгой формализации предложенных концептуальных подходов.

Автор выражает искреннюю признательность проф. А.Е. Барановичу за постановку задачи, ценные методические указания и неоценимую поддержку и помощь в научной работе.

Аббревиатуры

АИС – антропоморфная интеллектуальная система
ВИ – вербальная информация
МТ – музыкальный текст
ПП – прагматический потенциал
С.С. – строгий стиль

Примечания

[1] См.: *Бонфельд М.Ш.* Музыка: Язык. Речь. Мышление. Опыт системного исследования музыкального искусства. Вологда, 1999.

[2] См.: *Арановский М.Г.* Музыкальный текст: структура и свойства. М.: Композитор, 1998.

[3] См.: *Баранова. С.Ю.* Музыкальный текст: язык, знак, сигнал, символ // Электронный научный журнал «Вестник Омского государственного педагогического университета». Вып. 2007. [Электронный ресурс] [М., 2011] // URL.: http:// omsk.edu/article/vestnik-omgpu-173.pdf (дата обращения: 06.02.2012).

[4] См.: *Зарипов Р.Х.* Кибернетика и музыка. М.: Знание, 1963; см.: *Зарипов Р.Х.* Машинный поиск вариантов при моделировании творческого процесса. М.: Наука; Гл. ред. физ.-мат. лит-ры, 1983.

[5] См: *Адамов Г.Б.* Тайна двух океанов. М.: ЭКСМО, 2007.

[6] См.: *Baranovich A.E.* Pragmatic potential of verbal information: aspects of mathematical modeling / Proc. of the 12th Intern. Conf. “Speech and Computer” SPECOM’2007. Vol. 2. Moscow, 2007. P. 844–852.

[7] См.: *Баранович А.Е., Иглицкая С.М.* О некоторых результатах сравнительного анализа музыкального и вербального текстов / Материалы X Междунар. конф. «Интеллектуальные системы и компьютерные науки». М.: МГУ, 2011 (в печати).
См.: *Иглицкая С.М.* К вопросу структурно-алгебраического и семантико-прагматического анализа музыкального текста // Вестник РГГУ. 2011. № 13/11. С. 128–145. Сер. «Информатика. Защита информации. Математика».

[8] См.: *Баранович А.Е.* Семиотико-хроматические гипертопографы. Введение в аксиоматическую теорию: информационный аспект. М.: ГШ ВС РФ, 2003.

[9] См.: *Баранович А.Е.* Семиотико-хроматические гипертопосети: унифицированная модель представления знаний / Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2011): Материалы Междунар. научн.-техн. конф. Минск: БГУИР, 2011. С. 71–86.

[10] См.: *Баранович А.Е.* Семантические аспекты информационной безопасности: концентрация знаний // Вестник РГГУ. 2011. № 13/11. С. 38–58. Сер. «Информатика. Защита информации. Математика».

[11] См. *Баранович А.Е.* Многоосновные СХ-гипертопографы – однообъектная парадигма / Тр. III Междунар. конгресса по интеллект. системам и информ. технол. / XI Междунар. научн.-техн. конф. «Интеллектуальные системы» (AIS’11). М.: Физматлит, 2011. Т. 1. С. 377–385.

[12] См.: *Мазель Л.А., Цуккерман В.А.* Анализ музыкальных произведений. М.: Музыка, 1967.

[13] См.: Музыкальная энциклопедия: В 6 т. Т. 5. Советская энциклопедия, 1981.

[14] См.: *Фраенов В.П.* Учебник полифонии. М.: Музыка, 1987.

[15] См.: The Mutopia Project: Free sheet music for everyone [Электронный ресурс]. [M., 2011]. URL.: http://mutopiaproject.org (дата обращения: 06.02.2012). См.: LilyPond... music notation for everyone [Электронный ресурс]. [M., 2011]. URL: http://lilypond.org (дата обращения: 06.02.2012).

А.Н. Приезжая

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Процесс разработки информационной системы в защищенном исполнении требует трудоемкого анализа защищаемого объекта и разработки большого количества документации. В данной статье предлагается технология, основанная на автоматизированном преобразовании моделей, которая позволяет одновременно разрабатывать несколько представлений объекта, включая модели угроз и нарушителя и в автоматизированном режиме строить на их основе модель информационной системы в защищенном исполнении.

Ключевые слова: UML-модель, автоматизация, разработка автоматизированной системы, преобразование моделей, модель объекта.

В России существует огромное количество видов (категорий) информации, подлежащей защите (по некоторым оценкам до 30), и к каждому из них предъявляются свои требования по обеспечению безопасности[1], кроме того в связи с развитием информационных технологий постоянно растет сложность систем обработки данных. В результате специалисты в области информационной безопасности сталкиваются с необходимостью защищать все более сложные системы в соответствии с разными, порой противоречивыми требованиями, и при этом сроки разработки СЗИ крайне ограничены. В связи со всем вышесказанным особую актуальность приобретает создание средств поддержки разработки защищенных систем.

Рассматриваемый метод автоматизированной разработки информационных систем в защищенном исполнении включает

в себя разработку нескольких взаимосвязанных формальных моделей объекта, предназначенных для автоматизированного преобразования. В рамках данной статьи процесс разработки информационных систем в защищенном исполнении рассматривается применительно к информационным системам обработки персональных данных.

В соответствии с ГОСТ Р 51583-2000[2] и ГОСТ 34.601[3] разработка информационных систем в защищенном исполнении осуществляется следующим образом:

– формирование требований к информационной системе, в том числе обследование объекта защиты, определение факторов влияющих на информацию, разработка предварительных требований по защите информации;

– разработка концепции АС, в том числе формирование модели угроз информационной системы, определение принципов построения системы защиты;

– разработка технического задания на создание информационной системы в защищенном исполнении;

– разработка проектных решений (данная стадия может подразделяться на эскизное и техническое проектирование, разработку рабочей документации).

Далее следуют этапы по созданию и вводу в действие информационной системы в защищенном исполнении.

В данной статье рассматривается методика автоматизированного проектирования информационных систем в защищенном исполнении. Данная методика позволяет осуществлять разработку и документирование систем защиты информации в соответствии с ГОСТ 34 серии и нормативно-методическими документами ФСТЭК России и ФСБ России, регламентирующими обеспечение безопасности персональных данных и иной информации ограниченного доступа, не составляющей государственную тайну.

В соответствии с рассматриваемой методикой, проектирование информационных систем в защищенном исполнении осуществляется в несколько этапов:

– анализ информационной системы (определение актуальных угроз безопасности информационной системы и формирование требований к системе защиты информации);

– определение технического решения по защите информации (формирование модели защиты, определение состава применяемых средств и методов защиты);

– проверка решения на соответствие требованиям.

В процессе разработки информационной системы в защищенном исполнении формируется ряд прикладных моделей, характеризующих особенности конкретного объекта защиты (информационной системы). При формировании прикладных моделей используются базовые модели, содержащие структурированную информацию, в том числе описания угроз безопасности, возможностей нарушителя, средств защиты.

Рассматриваемая методика подразумевает автоматизированную разработку, т. е. формирование прикладных моделей средствами автоматизации на основании введенных данных. Вместе с тем предлагаемая методика подразумевает возможность корректировки полученных данных экспертом в области защиты информации, что позволяет обеспечить большую гибкость и адаптивность системы.

Рассмотрим процесс проектирования информационных систем в защищенном исполнении более детально.

Для определения необходимых и достаточных мер защиты информационных систем формируется модель угроз безопасности информационной системы. В ходе формирования модели угроз выявляется перечень угроз, актуальных для конкретной информационной системы. Модель угроз безопасности формируется на основе анализа объекта защиты – информационной системы.

При этом для определения перечня актуальных для конкретной информационной системы угроз безопасности необходимо провести анализ уязвимостей системы и возможностей нарушителя, т. е. сформировать прикладную модель нарушителя. При определении возможных атак необходимо учитывать, что атака, реализующая ту или иную угрозу, может происходить в несколько этапов, т. е. помимо защищаемых ресурсов должны быть определены потенциальные точки воздействия – элементы объекта защиты, посредством которых может быть проведена атака на защищаемую информацию.

Прикладная модель нарушителя в сочетании с прикладной моделью объекта определяет перечень возможных угроз безопасности информации; данный перечень может быть скорректирован экспертом в части уточнения потенциального ущерба и вероятности реализации угроз, после чего формируется перечень актуальных угроз безопасности – прикладная модель угроз.

Таким образом, в ходе анализа информационной системы должны быть сформированы следующие прикладные модели: модель объекта защиты; модель нарушителя; модель угроз.

Подробное описание формирования вышеуказанных моделей дано в статье «Автоматизированное формирование модели угроз безопасности информационной системы»[4].

На основе прикладной модели угроз формируются требования к защите рассматриваемой информационной системы. При формировании перечня требований к системе защиты используется следующее правило: «Каждой актуальной угрозе безопасности должно соответствовать как минимум одно требование к методу (средству) противодействия». Требования к системе защиты информации в свою очередь определяют состав применяемых средств и мер защиты, которые описываются прикладной моделью защиты. Модель защиты должна предлагать способ нейтрализации для всех актуальных способов доступа.

Рассмотрим формирование модели защиты. Для ее формирования используются следующие базовые модели:

– модель «Возможности средств защиты»;

– модель «Типовые решения»;

– модель «Обязательные средства защиты».

Базовая модель «Возможности средств защиты» описывает функциональные возможности средств защиты, в том числе для каждой возможности средств защиты, а также для каждого СрЗИ указываются иные параметры выбора, такие как стоимость и наличие сертификатов соответствия, недостатки (например, сложность администрирования).

В рамках данной статьи рассматривались следующие механизмы защиты:

организационные меры защиты;

технические средства защиты:

средства защиты от утечки по техническим каналам;

средства управления доступом;

средства регистрации и учета;

средства контроля целостности;

средства межсетевого экранирования;

средства защиты от утечек и несанкционированного распространения информации;

средства обнаружения атак;

средства анализа защищенности;

средства криптографической защиты;

средства антивирусной защиты;

средства централизованного управления.

Структура базы данных, содержащей модель «Возможности средств защиты» приведена на рис. 1.

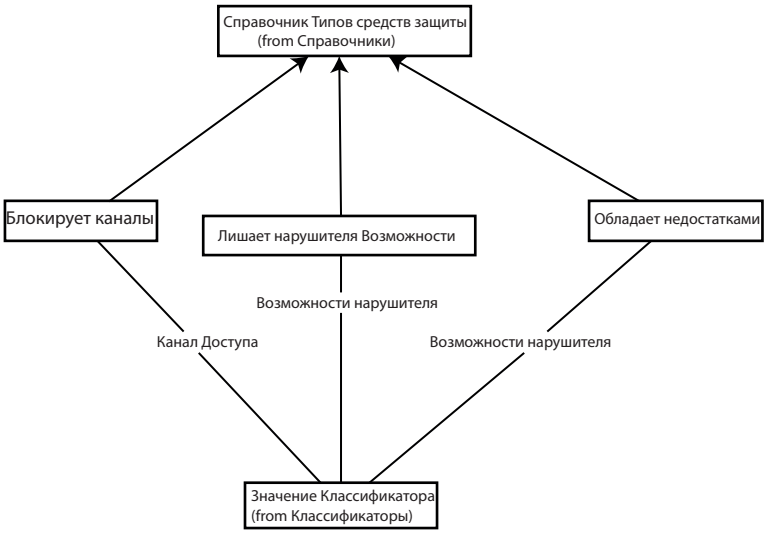


Рис 1. Структура базы данных «Возможности средств защиты»

Базовая модель «Типовые решения» описывает наборы технических средств и организационных мероприятий, достаточных для противодействия конкретной угрозе при условии ограничений. Подобный набор может быть сформирован как на основе нормативно-методических документов в области информационной безопасности (требований к классам защищенности), так и на основе предшествующего опыта. Модель «Типовые решения» используется для разработки прикладной модели «Средства защиты».

Структура базы данных, содержащей модель «Типовые решения», приведена на рис. 2.

При этом «Документ» определяет нормативно-методические, проектные решения, в соответствии с которыми это типовое решение сформировано, что позволяет эксперту дополнительно оценить его применимость в данном случае.

Также при формировании прикладной модели «Средства защиты» используется базовая модель «Обязательные средства защиты» (рис. 3), описывающая наборы технических средств

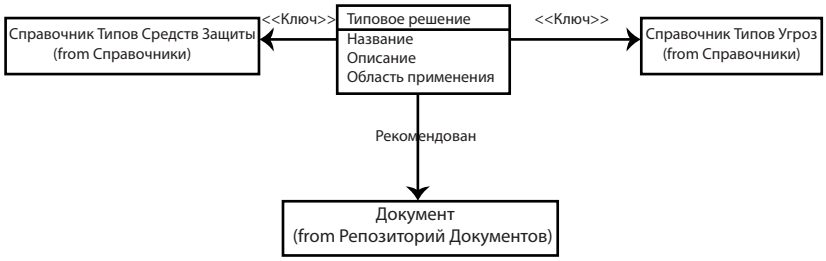


Рис 2. Структура базы данных, содержащей модель «Типовые решения»

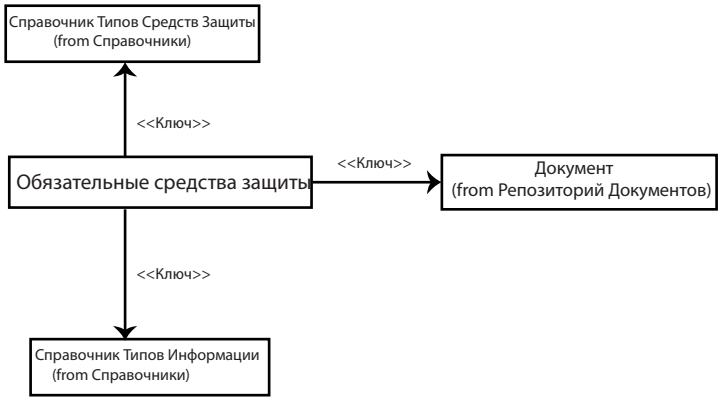


Рис 3. Структура базы данных, содержащей модель «Обязательные средства защиты»

и организационных мероприятий, рекомендованных для использования в нормативно-методических документах регуляторов в области информационной безопасности в системах, обрабатывающих определенные типы информации.

Собственно формирование прикладной модели защиты разбивается на следующие этапы:

– выбор средств защиты от актуальных угроз;

– встраивание средств защиты в структуру объекта защиты;

– проверка достаточности предложенных мер, разработка дополнительных рекомендаций по использованию средств защиты информации и организационных мер.

На основании прикладных моделей угроз и объекта защиты определяются защищаемые ресурсы и потенциальные точки воздействия (элементы объекта защиты, посредством которых может быть проведена атака на защищаемую информацию), для которых необходима реализация защиты. Для каждого ресурса и потенциальной точки воздействий автоматически определяется перечень подключаемых механизмов (средств) защиты, также при выборе средств защиты учитываются дополнительные параметры в зависимости от выставленного экспертом приоритета (например, минимальная стоимость решения или максимальная надежность используемых средств).

При встраивании средств защиты в структуру объекта защиты используется модель контуров защиты. При этом контур защиты определяется следующим образом:

Контур защиты объединяет один или несколько элементов объекта защиты.

В контуре защиты могут быть применены одно или несколько средств защиты, которые не позволяют нарушителю воспользоваться теми или иными каналами реализации угрозы или лишить его возможности реализовать другие возможности в отношении принадлежащих контуру элементов системы. Защитные возможности контура являются объединением возможностей средств, описанных в справочнике средств защиты (формируются автоматически на основе базовой модели).

Примерами контура защиты могут служить:

– контролируемая зона, лишающая внешнего нарушителя возможности физического доступа и использования ПЭМИН;

– организационные мероприятия, исключающие возможности сговора с внутренним нарушителем;

– АРМ с установленными средствами защиты от НСД;

– сеть с межсетевым экраном.

В процессе разработки контуров защиты эксперт имеет возможность производить автоматическую оценку актуальных угроз с учетом контуров защиты. Угрозы, реализуемые в условиях применения средств защиты, получаются аналогично перечню актуальных угроз безопасности информационной системы. Данная прикладная модель может быть использована в дальнейшем при сопровождении информационной системы, в том числе и для оценки защищенности информационной системы при ее модернизации.

Контуры защиты являются достаточно универсальным механизмом описания средств и мер по защите информации. Однако

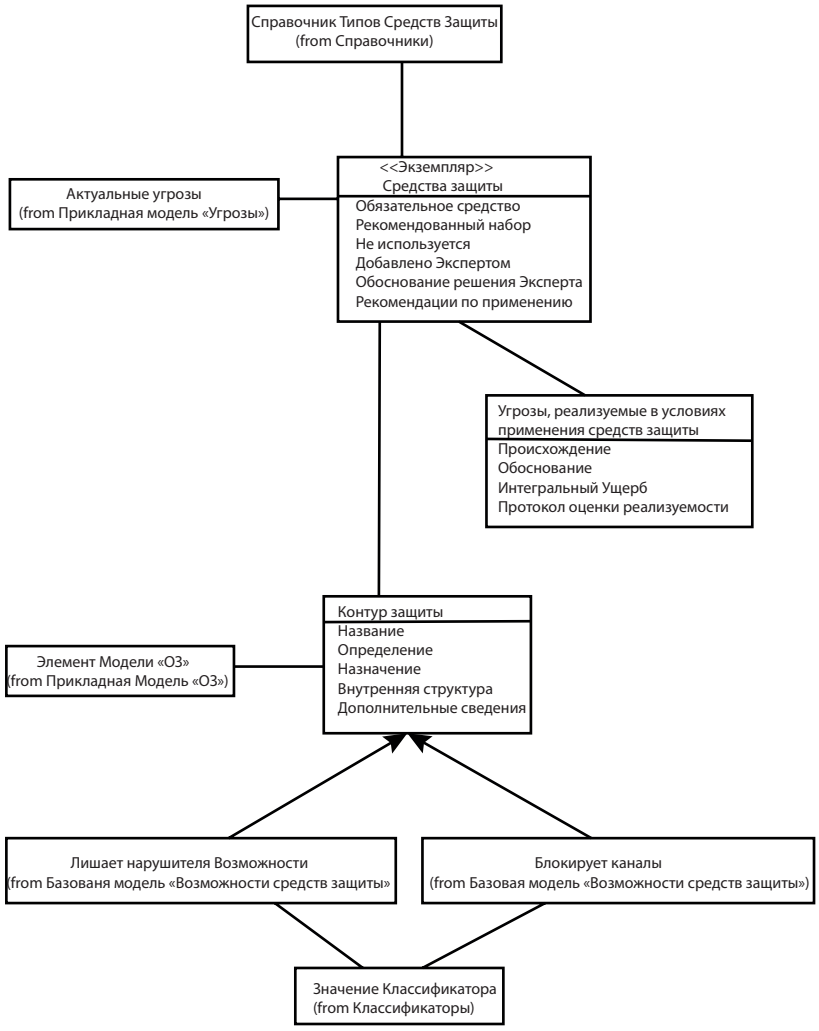


Рис 4. Структура прикладной модели защиты

в тех случаях, когда эксперт сочтет этот механизм неудобным, он может сформулировать свои рекомендации по защите от «угроз, реализуемых в условиях применения средств защиты», в свободной форме.

Подготовка рекомендаций по использованию средств защиты осуществляется в автоматическом режиме с использованием базовых моделей «Обязательные средства защиты» и «Типовые решения». При этом формируется общий список рекомендованных средств защиты, в котором для каждого средства указаны:

1) происхождение данного средства:

– типовое решение (с указанием списка названий типовых решений, рекомендующих использование данного средства);

– обязательное средство (со ссылкой на документы, предписывающие их применение);

– добавлено экспертом (с обоснованием данного средства);

2) информация о решениях эксперта и их обосновании:

– эксперт может отказаться от использования рекомендованного средства;

– заменить рекомендованное средство на аналогичное (того же типа), выбранное из справочника средств защиты;

3) информация об использовании данного средства. При этом возможно два варианта использования:

– средство может быть использовано в одном или нескольких контурах защиты;

– эксперт может дать рекомендации по применению данного средства в свободной форме.

Предлагаемые средства защиты включаются в прикладную модель объекта, формируя модель информационной системы в защищенном исполнении. На данном этапе проводится проверка достаточности предложенных средств защиты. Достаточность определяется на основании повторной генерации модели угроз: если предложенные средства защиты обеспечивают противодействие всем актуальным угрозам безопасности, генерация выдаст пустое множество атак, иначе требуется экспертное решение (например, переоценка ущерба, наносимого данной угрозой, или поиск альтернативного решения по защите).

По результатам построения модели защиты формируется перечень рекомендуемых мер и средств защиты.

При формировании прикладной модели «Средства защиты» используются следующие правила:

– для каждого требования должно быть предусмотрено средство защиты, его выполняющее;

– для каждой потенциальной точки воздействия должно быть предусмотрено средство защиты;

Таблица

Описание алгоритма

Шаг	Действие
Автоматическое формирование требований и рекомендаций по защите	Подготовка рекомендаций по использованию средств защиты осуществляется в автоматическом режиме с использованием базовых моделей «Обязательные средства защиты» и «Типовые решения»
Корректировка рекомендаций экспертом	Эксперт может: – отказаться от использования рекомендованного средства; – заменить рекомендованное средство на аналогичное, выбранное из справочника средств защиты; – добавить средство из справочника средств защиты. Во всех случаях эксперт должен привести обоснование принятого решения
Формирование контура(ов) защиты	При встраивании средств защиты в структуру ОЗ используется модель контуров защиты: – контур защиты содержит один или несколько элементов ОЗ; – в контуре защиты может применено одно или несколько средств защиты, которые не позволяют нарушителю воспользоваться теми или иными каналами реализации угрозы или лишить его возможности реализовать те или иные возможности в отношении принадлежащих контуру элементов системы. Защитные возможности контура являются объединением возможностей средств, описанных в справочнике средств защиты (формируются автоматически)
Оценка реализуемых угроз при наличии контуров защиты и использовании типовых решений	Производится автоматически
Обеспечена защита от всех актуальных угроз	Если в результате оценки реализуемости угроз с учетом средств защиты выявлены актуальные угрозы, то процесс повторяется начиная с этапа 3.
Формирование отчета по принятым экспертом решениям и их обоснованиям	Автоматически формируемый отчет содержит информацию о принятых экспертом решениях: – отказах от использования рекомендованного средства; – заменах рекомендованных средств на аналогичные; – использовании дополнительных средств защиты

– подтип угрозы наследует все средства и меры защиты, рекомендованные для угроз, расположенных выше по иерархии.

Описание алгоритма проектирования информационной системы в защищенном исполнении приведено в таблице.

Требования к системам защиты информации формулируются не только заказчиком, но и государственными регуляторами в сфере информационной безопасности. Одной из проверок реализованной прикладной модели защиты является проверка достаточности функциональных возможностей выбранных средств защиты для выполнения требований регуляторов, применяемых к данному классу систем (класс системы определяется в прикладной модели объекта на основании характеристик объекта и нормативно-методических документов проекта). Требования по составу и функциям средств защиты в соответствии с требованиями регуляторов фиксируются в модели «Обязательные средства», проверка осуществляется путем сравнения полученной модели с требованиями для данного класса.

Предложенный подход упрощает анализ системы, сокращает затраты времени на рутинные процедуры и снижает вероятность ошибки, иными словами, снижает финансовые и временные затраты на разработку защищенной системы, что позволяет существенно сократить сроки и стоимость разработки системы защиты информации, в том числе за счет автоматизированной генерации документов проекта на основании шаблонов, так как формализация описания как объекта защиты, средств защиты и иных значимых для проектирования системы защиты информации сущностей является неотъемлемой частью данного подхода. Задача генерации документов на основании моделей может быть осуществлена с использованием общепринятых подходов к генерации документов на основе элементов базы знаний.

Примечания

[1] См.: *Ефремов А.* Понятие и виды конфиденциальной информации. [Электронный ресурс] // Новостной сайт «CNews». [М., 2007]. URL: http://www.russianlaw.net/law/doc/a90.htm (дата обращения: 06.02.2012).

[2] См.: ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. [Электронный ресурс] [М., 2000]. URL: http://www.ispdn.narod.ru/gost2000.pdf (дата обращения: 06.02.2012).

[3] См.: ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания». // Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. М.: Издательство стандартов, 2000.

[4] См.: *Приезжая А.Н.* Автоматизированное формирование модели угроз безопасности информационной системы // Вестник РГГУ. 2012. № 14/12. Сер. «Информатика. Защита информации. Математика». (в печати)

А.С. Платонова

ПРОЕКТИРОВАНИЕ БАЗЫ ДАННЫХ ДЛЯ ИНФОРМАЦИОНОЙ СИСТЕМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБРАЗОВАНИЯ

Статья посвящена проектированию базы данных, предназначенной для упорядоченного хранения психолого-педагогической информации, полученной по итогам контроля и оценивания результатов образования: учебного и контрольно-измерительного материалов, ответов обучаемых, записей учителей и различного рода служебной информации. Проектирование структуры хранения информации осуществлено на уровнях концептуального, логического и физического проектирования баз данных, в результате построен комплекс взаимосвязанных моделей базы данных.

Ключевые слова: контроль и оценка результатов образования, хранение психолого-педагогической информации, база данных, семантическая модель, даталогическая модель, MySQL, физическая модель.

Проектирование базы данных (БД) осуществляется в рамках разработки информационной системы (ИС) контроля и оценки результатов образования (на примере среднего образования). Совершенствование, или по крайней мере дополнение, традиционных средств контрольно-оценочной деятельности в школе на сегодняшний момент является весьма актуальной задачей[1]. ИС предназначена для осуществления автоматизированной контрольно-оценочной деятельности (КОД) в школе и обеспечивает ввод, хранение, обработку и представление информации об образовательных результатах учащихся.

Разрабатываемая система отличается тем, что осуществляет автоматизированный контроль предметных знаний и умений школьников на различных уровнях усвоения учебного материала,

надпредметных умений и навыков, а также характеристик личностного развития и воспитанности. Кроме того, по итогам контроля система предоставляет не просто итоговые баллы, а, во-первых, интегративную оценку достигнутого уровня результатов образования любого из учащихся, представляющую собой подробную психолого-педагогическую характеристику школьника; во-вторых, различного рода статистическую информацию по отдельному ученику, классу, параллели в виде таблиц и графиков, предназначенную главным образом для администрации школы[2]. Наполнение интегративной оценки зависит от того, какой пользователь запросил ее формирование: ученик и родитель или учитель и психолог[3].

Перед проектированием БД нами были реализованы все этапы создания информационных систем, в том числе разработаны архитектура, в основе которой лежит трехзвенная архитектура клиент-сервер, и функциональная модель ИС, построенная с использованием графических нотаций IDEF0 и DFD[4]. Это позволило перейти к проектированию БД с целью реализации упорядоченного хранения всей необходимой информации, возможности получения данных по запросам, сокращения избыточности и дублирования данных, обеспечения целостности данных. В ходе проектирования базы данных реализованы этапы концептуального, логического и физического проектирования. В результате построен комплекс взаимосвязанных моделей БД.

В статье рассказывается о разработке части базы данных, предназначенной для хранения информации, связанной с контролем умения учащихся решать задачи по физике. Ученик в режиме диалога с компьютером выполняет контрольную работу, состоящую из задач различного уровня сложности. Решение задачи заключается в выполнении ряда этапов, начиная с записи краткого условия и заканчивая вводом ответа. Выполнение каждого из этапов представляет собой решение тестового задания с выбором одного варианта из нескольких предложенных.

В рамках проектирования БД на концептуальном уровне построена семантическая (инфологическая) модель «сущность–связь». Она представляет собой набор концепций, которые описывают структуру базы данных и связанные с ней транзакции обновления и извлечения данных. Модель «сущность–связь» наиболее известный представитель класса семантических моделей предметной области. Основными преимуществами моделей «сущность–связь» является наглядность, возможность проектирования базы данных с большим количеством объектов и атрибутов, реализо-

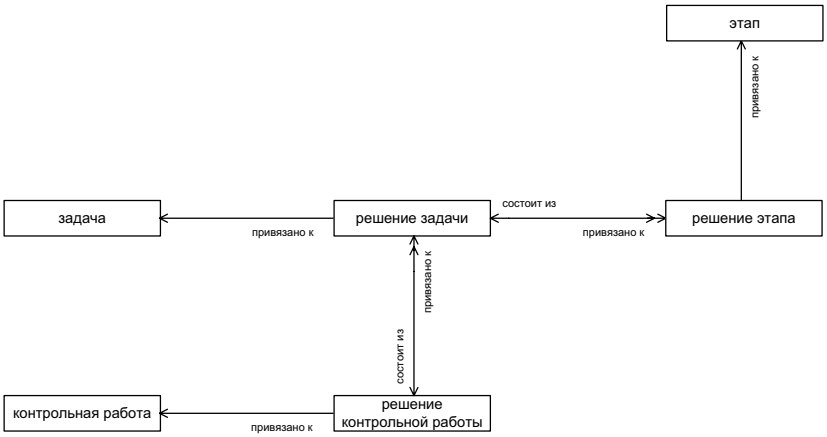


Рис.1. Фрагмент семантической модели БД

ванность во многих системах автоматизированного проектирования баз данных. Способ графического представления такой модели – графическая диаграмма ER. Построение диаграммы ER осуществлено с помощью графической нотации Баркера. Основными элементами ER-моделей являются:

– сущность, являющаяся классом однотипных объектов, информация о которых должна быть учтена в модели и имеющая наименование, выраженное существительным в единственном числе;

– экземпляр сущности как конкретный представитель данной сущности;

– ключ сущности – неизбыточный набор атрибутов, значения которых в совокупности являются уникальными для каждого экземпляра сущности;

– атрибуты сущностей – характеристика, являющаяся некоторым свойством сущности и имеющая наименование, выраженное существительным в единственном числе;

– связь – ассоциация между двумя сущностями, позволяет по одной сущности находить другие сущности, связанные с нею[5].

Фрагмент семантической модели БД представлен на рис. 1.

При разработке ER-модели нами выделены информационные сущности предметной области, атрибуты сущностей, взаимосвязи между сущностями. Основными сущностями базы данных являются:

– сущность «Задача»; характеризуется атрибутами: краткое условие, перевод в СИ, процесс, график, формулы, конечная формула, результат. Данная сущность связана с сущностью «Решение задачи»;

– сущность «Этап»; характеризуется атрибутами: название, балл. Данная сущность связана с сущностью «Решение этапа»;

– сущность «Контрольная работа»; характеризуется атрибутами: имя, количество задач, раздел. Данная сущность связана с сущностями «Решение контрольной работы»;

– сущность «Решение этапа»; характеризуется атрибутом: балл. Данная сущность связана с сущностями «Решение задачи» и «Этап задачи»;

– сущность «Решение задачи»; характеризуется атрибутами: дата, время, балл. Данная сущность связана с сущностями «Решение этапа», «Решение контрольной работы»;

– сущность «Решение контрольной работы»; характеризуется атрибутами: дата, время, балл. Данная сущность связана с сущностями «Контрольная работа», «Решение задачи».

По данной концептуальной схеме построена даталогическая диаграмма, которая будет учитывать такие особенности СУБД, как допустимые типы и наименования полей, таблиц.

Для построения даталогической модели из модели «сущность–связь» нами учитывались следующие правила:

1) каждая сущность превращалась в таблицу;

2) каждый атрибут сущности становился столбцом таблицы;

3) компоненты ключа сущности превращались в первичный ключ таблицы;

4) для отображения связи «один ко многим» («многие к одному») делалась копия ключевого атрибута (атрибутов) с конца связи «один», соответствующие столбцы составляли внешний ключ;

5) связи «многие ко многим» разбивались путем формирования трех отношений, по одному для каждой сущности, и третье, имеющее составной ключ, построенный из ключей первых двух;

6) указывались типы полей таблиц.

Даталогическая модель построена на основе реляционной модели данных. Существуют и другие типы моделей данных: иерархические, сетевые. Но на сегодняшний день реляционные модели данных наиболее распространены, хотя и обладают рядом недостатков. В реляционной модели достигается гораздо более высокий уровень абстракции данных, чем в иерархической или сетевой, описываются данные на основе только их естественной структуры,

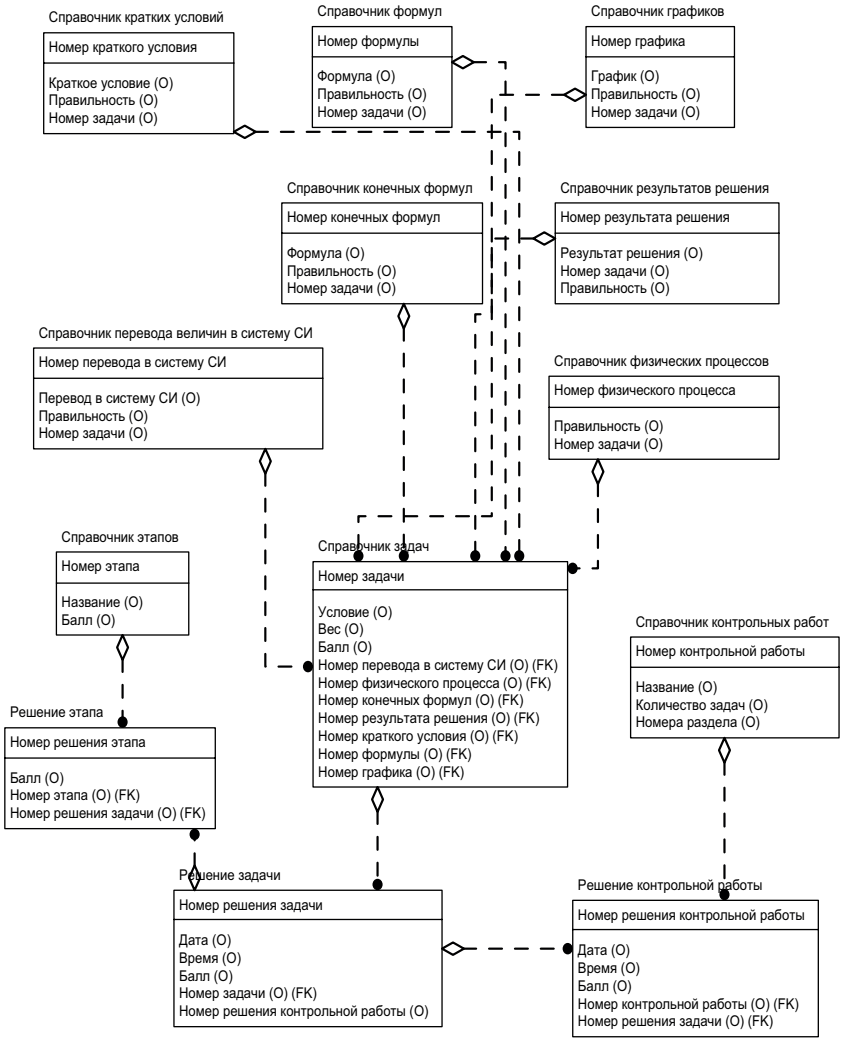


Рис. 2. Фрагмент даталогической модели БД

т. е. нет потребности введения какой-либо дополнительной структуры для целей машинного представления[6].

На рис. 2 представлен фрагмент даталогической модели БД.

Созданы следующие таблицы базы данных (табл. 1–14).

Таблица 1

Справочник кратких условий

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер краткого условия	Номер	Счетчик	Целое
	Краткое условие	Краткое условие	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 2

Справочник формул

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер формулы	Номер	Счетчик	Целое
	Формула	Формула	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 3

Справочник графиков

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер графика	Номер	Счетчик	Целое
	График	График	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 4

Справочник конечных формул

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер конечной формулы	Номер	Счетчик	Целое
	Формула	Конечная формула	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 5

Справочник переводов в СИ

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер перевода в СИ	Номер	Счетчик	Целое
	Перевод в СИ	Перевод в СИ	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 6

Справочник кратких условий

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер краткого условия	Номер	Счетчик	Целое
	Краткое условие	Краткое условие	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 7

Справочник процессов

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер процесса	Номер	Счетчик	Целое
	Физический процесс	Процесс	Текстовый	255
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 8

Справочник результатов

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер результата	Номер	Счетчик	Целое
	Результат	Результат	Числовой	Дробное
	Правильность	Правильность	Числовой	Целое
	Номер задачи	Номер_задача	Числовой	Целое

Таблица 9

Справочник этапов

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер этапа	Номер	Счетчик	Целое
	Название	Название	Текстовый	50
	Балл	Балл	Числовой	Дробное

Таблица 10

Справочник задач

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер задачи	Номер	Счетчик	Целое
	Условие	Условие	Текстовый	255
	Вес	Вес	Числовой	Дробное
	Балл	Балл	Числовой	Дробное
	Номер краткого условия	Номер_краткое условие	Числовой	Целое
	Номер перевода в СИ	Номер_перевод в СИ	Числовой	Целое
	Номер процесса	Номер_процесс	Числовой	Целое
	Номер графика	Номер_график	Числовой	Целое
	Номер формулы	Номер_формула	Числовой	Целое
	Номер конечной формулы	Номер_конечная формула	Числовой	Целое
	Номер результата	Номер_результат	Числовой	Целое

Таблица 11

Справочник контрольных работ

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер контрольной работы	Номер	Счетчик	Целое
	Название	Название	Текстовый	50
	Количество задач	Количество задач	Числовой	Целое
	Номер раздела	Номер_раздел	Числовой	Целое

Таблица 12

Решение этапа

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер решения этапа	Номер	Счетчик	Целое
	Балл	Балл	Числовой	Дробное
	Номер решения задачи	Номер_решение задачи	Числовой	Целое

Таблица 13

Решение задачи

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер решения задачи	Номер	Счетчик	Целое
	Балл	Балл	Числовой	Дробное
	Дата	Дата	Дата	
	Время	Время	Время	
	Номер решения контрольной работы	Номер_решение контрольной работы	Числовой	Целое

Таблица 14

Решение контрольной работы

Код	Наименование	Идентификатор	Тип поля	Размер
*	Номер решения контрольной работы	Номер	Счетчик	Целое
	Балл	Балл	Числовой	Дробное
	Дата	Дата	Дата	
	Время	Время	Время	
	Номер контрольной работы	Номер_контрольная работа	Числовой	Целое
	Номер решения задачи	Номер_решение задачи	Числовой	Целое

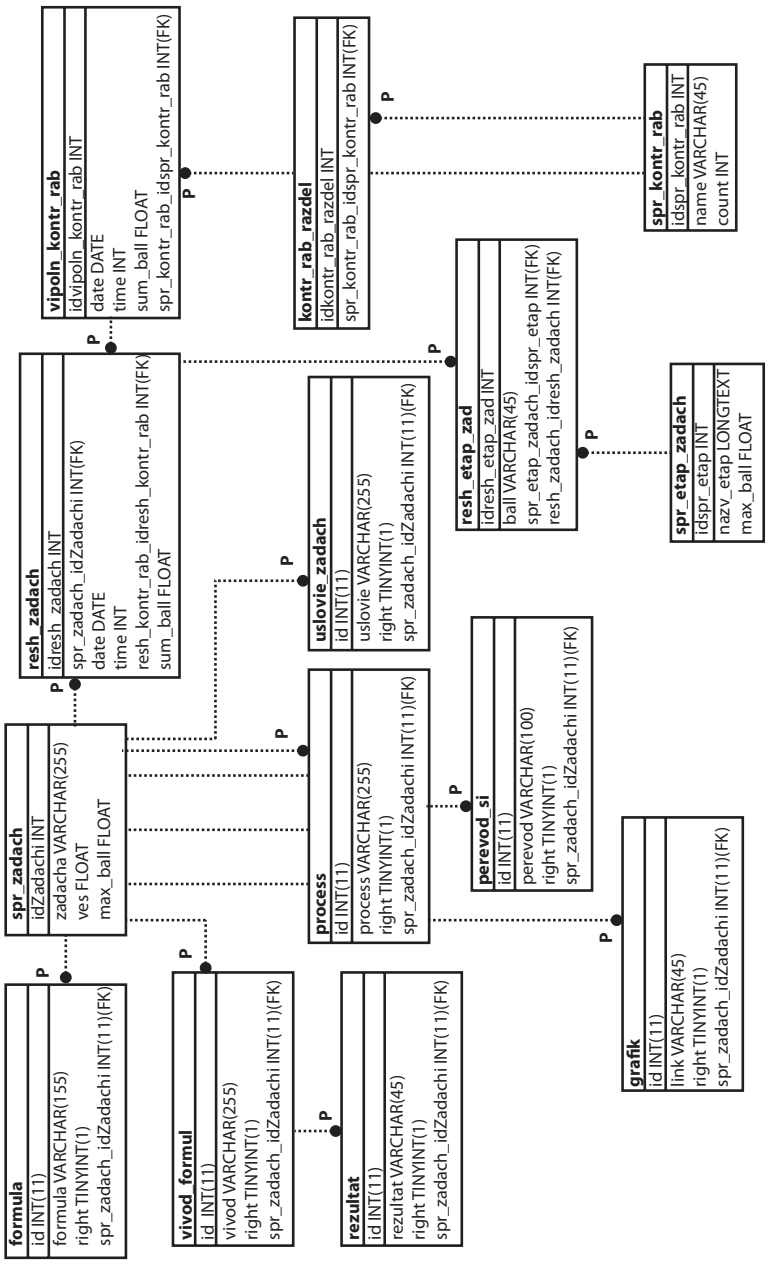


Рис. 3. Фрагмент физической модели БД

Физическая модель БД построена в СУБД MySQL. MySQL – это реляционная система управления базами данных и является наиболее приспособленной для применения в среде web. То есть данные в ее базах хранятся в виде логически связанных между собой таблиц, доступ к которым осуществляется с помощью языка запросов SQL. MySQL – свободно распространяемая система, платить за ее применение не нужно. Кроме того, это достаточно быстрая, надежная и, главное, простая в использовании СУБД, вполне подходящая для не слишком глобальных проектов[7]. Работать с MySQL можно не только в текстовом режиме, но и в графическом. Для моделирования таблиц базы данных и связей между ними использовалась среда MySQLWorkbench. Программа генерирует скрипт для создания таблиц в СУБД MySQL.

Здесь уточнены типы атрибутов согласно выбранной СУБД. Все сущности и их атрибуты записаны с помощью букв латинского алфавита. Индексные поля автоматически создаются по ключевым полям. Фрагмент физической модели БД в среде MySQLWorkbench представлен на рис. 3.

Таким образом, база данных, спроектированная на концептуальном, логическом и физическом уровнях, позволяет организовать упорядоченное хранение учебного, контрольно-измерительного материалов, ответов учащихся, записей учителей, служебной информации, необходимой для функционирования приложений, и перейти непосредственно к разработке процедур ввода информации от пользователей системы, алгоритмов обработки результатов контроля, хранящихся в БД, алгоритмов предоставления участникам КОД полученной информации в виде интегративной оценки достигнутого уровня результатов образования любого из учащегося или графиков и таблиц со статистической информацией об отдельном ученике, классе или параллели.

Примечания

[1] См.: *Платонова А.С., Рыжкова М.Н.* Совершенствование методологии и методики оценивания учебных достижений учащихся // Системный анализ в науке и образовании: Электрон. науч. журнал. № 3 [Электронный ресурс]. [Дубна, 2010]. URL: http://www.sanse.ru/archive/17 (дата обращения 21.08.2011).

[2] См.: *Платонова А.С.* Информационное обеспечение педагогической инновации при усвоении курса физики // Инновации в образовании. 2011. № 2. С. 48–64.

[3] См.: *Платонова А.С.* О создании информационной системы контроля и оценки результатов школьного образования // Информационные технологии и информационная безопасность в науке, технике и образовании «ИНФОТЕХ-2011»: Материалы Междунар. науч.-тех. конф. Севастополь (Украина), 5–10 сент. 2011 г. Севастополь: СевНТУ, 2011. С. 232.

[4] См.: *Платонова А.С., Самохин А.В.* Проектирование информационной системы контроля и оценки образовательной деятельности учащихся: архитектура, модель и структура базы данных // Информационные системы и технологии. Орел: Орловский ГТУ, 2011. № 3 (65). С. 13–21.

[5] См.: *Пушников А.Ю.* Введение в системы управления базами данных. Ч. 1. Реляционная модель данных [Электронный ресурс]: Учеб. пособие. Уфа: Башкир. ун-т, 1999. 108 с. URL: http://citforum.ru/database/dblearn/dblearn08.shtml (дата обращения: 09.09.2011).

[6] Информационные технологии / О.Л. Голицына, Н.В. Максимов и др. М.: Инфра-М, 2009. С. 269.

[7] См.: Базы данных: основные понятия [Электронный ресурс]. URL: http://www.webmasterwiki.ru/MySQL (дата обращения 21.08.2011).

А.А. Пупыкина

ГРАФОВАЯ СТРУКТУРА СВЯЗАННЫХ МОДУЛЕЙ ПРИ ПРОЕКТИРОВАНИИ МОДЕЛИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ОБУЧАЮЩЕЙ СРЕДЫ

На основе требований, предъявляемых к методам проектирования пользовательского интерфейса обучающей среды, предложена модель обучающей среды, представленная в виде системы связанных модулей, образующих графовую структуру. Для проектирования средств адаптации пользовательского интерфейса предложено использовать когнитивные карты состояний.

Ключевые слова: граф, когнитивная карта состояний, модель, модельно ориентированный подход, обучающая среда, пользовательский интерфейс.

В последнее время широкое распространение получили информационные системы в обучении, реализующие новые образовательные технологии и создающие новую электронную обучающую среду. Эффективность обучающей среды в целом во многом обусловливается рядом факторов, одним из которых является эффективность и качество используемых средств обеспечения взаимодействия преподавателя и обучаемого. В электронной обучающей среде это пользовательский интерфейс (ПИ), который наряду с обучающим контентом – залог оптимальной обучающей среды.

Информация представляется пользователю через элементы ПИ (метафоры, выразительные средства) и механизмы организации взаимодействия с пользователем. Разнообразие современных технологических платформ создания ПИ, реализующих свои

варианты механизмов организации взаимодействия и метафор, приводит к проблемам переносимости интерфейсов между различными платформами. Переход на новую платформу ведет к полной повторной разработке. Для обучающих сред также важна постоянная работа над обучающим контентом, повышение наглядности материала и интерактивости. Это приводит к необходимости использования средств автоматизации проектирования ПИ, применяющих специализированные предметно ориентированные модели.

Современные системы автоматизации разработки ПИ ориентированы на конкретные платформы и технологии. Использование таких подходов разработки ПИ ведет к снижению трудоемкости процесса кодирования. Модельно ориентированные средства разработки ПИ кроме снижения трудозатрат на кодирование позволяют формировать проектные спецификации ПИ в виде наглядных моделей и документировать процесс его разработки. Такие подходы используют собственные графические языки описания ПИ или расширяют графические нотации проектирования приложений (например, UML). Одним из недостатков таких подходов является отсутствие средств выявления ошибок на этапе проектирования. Существуют виды ошибок, которые можно выявить и предотвратить на ранних этапах проектирования. К таким ошибкам можно отнести тупиковые сценарии человеко-компьютерного взаимодействия, недоступность компонентов пользовательского интерфейса. Предотвращение такого рода ошибок возможно с использованием средств методологий проектирования.

Разработка универсального модельно ориентированного подхода проектирования и разработки ПИ относится к достаточно сложному и трудоемкому классу задач. В то же время рассмотрение определенного класса программных систем позволит сузить круг решаемых проблем. К системам, для которых автоматизация проектирования и разработки ПИ важна и оправданна, можно отнести обучающие среды.

Для систем поддержки обучения характерен следующий список требований, предъявляемых к методам проектирования пользовательского интерфейса:

– наличие технологии оформления страниц экрана с применением графики, цвета, и пр.;

– возможность создания многоуровневой навигации в обучающей программе, т. е. возможен не только линейный (последовательный, шаг за шагом) порядок выполнения программы;

– наличие способов проектирования системы подсказок, ссылок на дополнительные материалы, выходы на иные информационные материалы;

– наличие средств разработки мотивирующих и информирующих сообщений;

– наличие способов создания средств взаимодействия пользователя с обучающей программой;

– наличие методов проектирования средств адаптации системы обучения к обучающемуся.

Рассмотрим способ проектирования ПИ обучающей среды, позволяющий организовать многоуровневую навигацию.

Модель обучающей среды можно представить в виде системы связанных модулей, образующих графовую структуру. Модулем может быть любой компонент системы. Изменение состояния i-го модуля с вероятностью Pij приведет к изменению состояния j-го модуля. Поэтому возникает необходимость отслеживать изменения в модулях, вызывающих изменения структуры обучающего материала, а вслед за ним и элементов пользовательского интерфейса, ответственных за его представление. Иерархичная структура обучающего материала может быть представлена в виде набора деревьев, имеющих перекрестные ссылки, что позволит создавать многоуровневую навигацию в обучающей программе, отражающую взаимосвязи различных учебных целей, задач и т. д.

Редактирование структуры учебного материала может приводить к:

– изменению элементов пользовательского интерфейса;

– изменению навигации в обучающей программе;

– отражению или сокрытию подсказок, ссылок на дополнительные материалы;

– генерации мотивирующих и информирующих сообщений.

Графовое представление обучающей среды позволяет определить число изменений, необходимых для внесения в систему, а также последовательность действий, приводящих к требуемому результату.

Для построения математической модели обучающей среды можно использовать иерархическую систему взаимосвязи модулей. Разработка модели обучающей среды может проводиться на нескольких уровнях абстракции, постепенно детализируя элементы модели до тех пор, пока не будет достигнут уровень, приемлемый для разработки элементов учебного материала $e_1, ..., e_n$ (n – количество элементов) на физическом уровне (рис. 1).

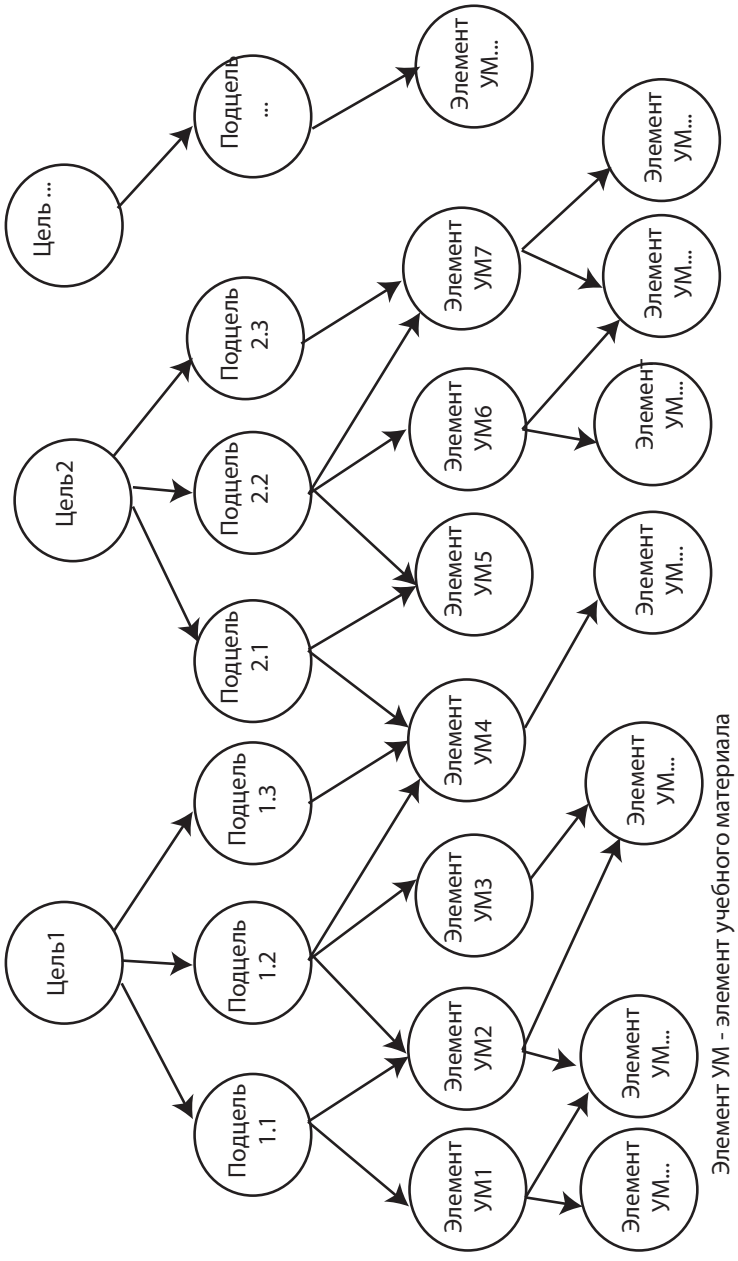


Рис. 1. Графовая структура взаимосвязанных модулей ПИ

Графовая структура взаимосвязанных модулей ПИ позволит также проектировать средства адаптации ПИ системы обучения к обучающемуся. Для этого на графе ПИ можно построить когнитивную карту ситуаций. Когнитивная карта ситуаций для модели обучающей среды позволит представить известные субъекту (преподавателю, создателю обучающего материала) основные закономерности наблюдаемой ситуации и предпочтительные траектории обучения в виде ориентированного знакового графа, в котором вершины графа – факторы (элементы учебного материала и показатели качества его прохождения обучающимся), а дуги между факторами – причинно-следственные связи между факторами. В когнитивной модели выделяют два типа причинно-следственных связей: положительные и отрицательные. При положительной связи увеличение значения фактора-причины приводит к увеличению значения фактора-следствия, а при отрицательной связи увеличение значения фактора-причины приводит к уменьшению значения фактора-следствия[1]. В модели обучающей среды с помощью причинно-следственных связей можно проектировать траектории обучения (рис. 2).

Предпочтительная траектория обучения описывает маршрут прохождения элементов учебного материала, приводящий к достаточному уровню освоения курса при высоких показателях качества выполнения контрольных заданий. Траектория обучения с увеличенным количеством дополнительных материалов описывает маршрут прохождения элементов учебного материала, расширенный подсказками, мотивирующими сообщениями, упражнениями для обеспечения достаточного уровня освоения курса при низких показателях качества выполнения контрольных заданий. В терминах когнитивной карты ситуаций предпочтительная траектория формируется за счет положительной причинно-следственной связи, траектория обучения с увеличенным количеством дополнительных материалов – за счет отрицательной. Таким образом, в зависимости от способностей ученика обучающая среда создает наиболее комфортный темп обучения. Это позволит обеспечивать адаптивность ПИ обучающей среды к обучающемуся, например, при высоком показателе качества выполнения контрольных заданий будут формироваться средства навигации на элементы учебного материала предпочтительной траектории обучения.

Для проектирования графовой структуры модулей ПИ обучающей среды необходимо определить систему элементов учебного материала $E = \{e_i\}$, $E = (I, Q)$, где $I = \{i_i\}$ – учебный контент, $Q = \{q_i\}$ – показатели качества прохождения обучения.

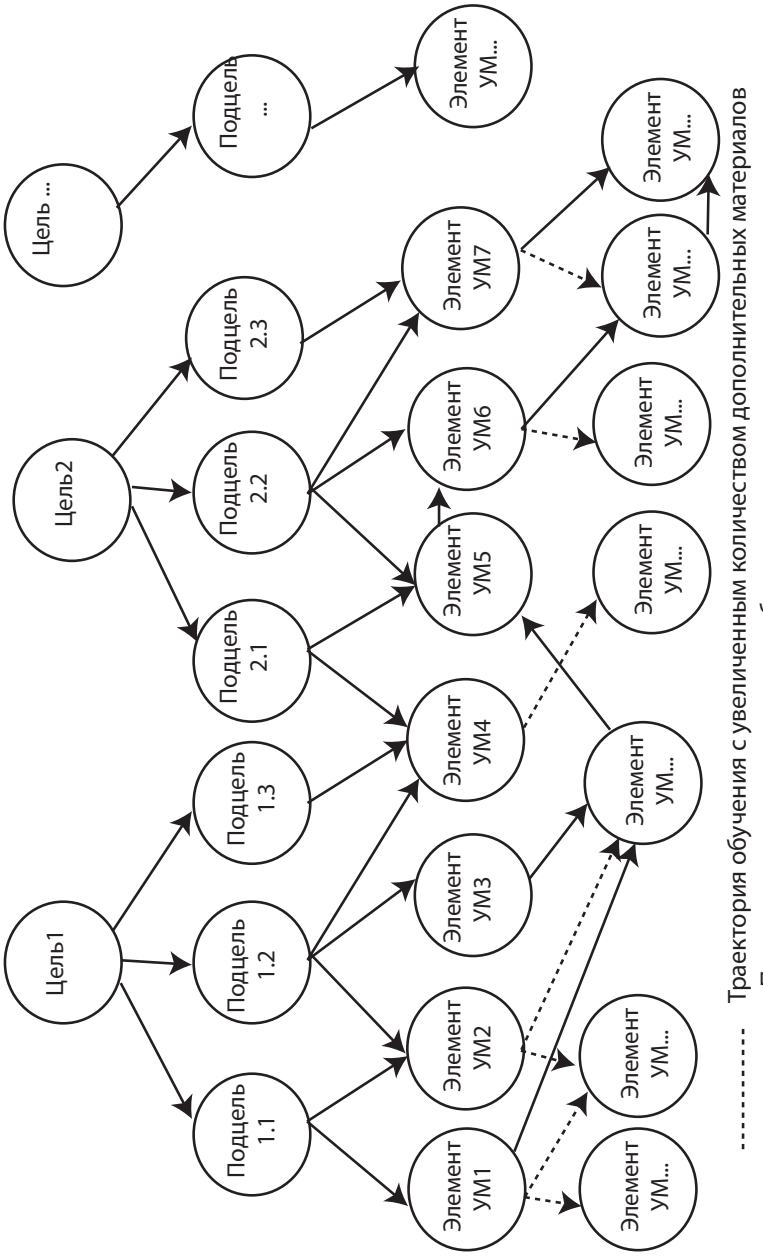


Рис.2. Траектории обучения в модели ПИ обучающей среды

Факторами когнитивной карты ситуаций примем значения q_i. Для каждого q_i необходимо определить показатели качества выполнения контрольных заданий в виде упорядоченного множества. Использование порядковых шкал значений в качестве измерительной системы позволит интегрировать в единую модель показатели качества, имеющие числовое и символьное представления.

Когнитивная карта ситуаций представляется в виде ориентированного знакового графа и задается матрицей смежности $W = \{w_{ij}\}$, $w_{ij} \in \{-1,0,1\}$.

Определяя силу взаимовлияния факторов, связанных причинными связями, знаковый орграф трансформируется во взвешенный орграф. Описание процессов перехода от одного фактора к другому осуществляется через систему уравнений «если... то...». В матричном виде такая система уравнений записывается в следующем виде[2]:

$$Z(t+1) = W^{\circ} Z(t)$$

где $Z(t) = (z_i(t))$ – начальный вектор приращений значений факторов в момент времени t; $Z(t+1) = (z_i(t+1))$ – вектор приращений значений факторов в момент времени $t+1$, $z_i(t) \in [-1,1]$; $W = |w_{ij}|$ – матрица смежности, $w_{ij} \in [-1,1]$ – характеризует силу причинной связи.

Приращения значений факторов в последовательные дискретные моменты времени $Z(t+1)$, ... , $Z(t+n)$ вычисляются с применением следующего правила композиции[3]:

$$z_i(t) = max(z_i^+(t), z_i^-(t)),$$

где $z_i^+(t) = \max\limits_j(z_i(t-1).\, w_{ij})$ – максимальное положительное, а $z_i^-(t)$ – максимальное по модулю отрицательное, $z_i^-(t) = \max\limits_j(|z_i(t-1).\, w_{ij}|)$ – приращение значения фактора-следствия.

Приращение значения фактора $z_i(t) \in Z(t)$, $\forall t$ представляется парой[4] $\langle z_i(t), c_i(t)\rangle$, где $c_i(t)$ – консонанс значения фактора $0 \le c_i(t) \le 1$:

$$c_i(t) = \frac{|z_i^+(t) + z_i^-(t)|}{|z_i^+(t)| + |z_i^-(t)|}.$$

Консонанс фактора характеризует уверенность субъекта в приращении значения $z_i(t)$ фактора q_i. При $c_i(t) \approx 1$, т. е. $z_i^+(t) >> |z_i^-(t)|$

или $|z_i^-(t)| >> z_i^+(t)$, уверенность субъекта в значении фактора qi(t) максимальна, а при $c_i(t) \approx 0$, т. е. $z_i^+(t) \approx |z_i^-(t)|$, минимальна. С помощью вычисления консонанса фактора можно адаптировать систему обучения к обучающемуся.

Таким образом, моделирование ПИ обучающей среды в виде графовой структуры взаимосвязанных модулей позволит проектировать многоуровневую навигацию, отслеживать случаи изменения структуры учебных материалов, приводящие к необходимости изменять ПИ, а также поддерживать систему адаптации среды к обучающемуся. Использование декларативного языка спецификации пользовательского интерфейса и средств автоматической генерации приведет к снижению стоимости и времени разработки обучающих сред. Модельно ориентированный подход к разработке интерфейса, предоставляющий автоматическую генерацию интерфейса по декларативным, высокоуровневым моделям интерфейса, позволит ослабить технологическую привязку разрабатываемого интерфейса к конкретной платформе.

Примечания

[1] См.: *Кулинич А.А.* Когнитивная система поддержки принятия решений «Канва» // Программные продукты и системы. 2002. № 3.

[2] Там же.

[3] См.: *Силов В.Б.* Принятие стратегических решений в нечеткой обстановке. М.: ИНПРО-РЕС, 1995.

[4] Там же.

О.В. Казарин

СОДЕРЖАНИЕ МОДЕЛЕЙ И МЕТОДОВ ПРОАКТИВНОЙ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В данной работе рассматриваются модели и методы проактивной защиты программного обеспечения информационной системы, под которой понимается защита, основанная на механизмах, учитывающих ее функциональные свойства, архитектурно-технологические особенности и характеристики внешней по отношению к системе среды на всех этапах жизненного цикла, предшествующих эксплуатации программ по назначению. В том числе на этапах, предшествующих этапам тестирования и испытания программ.

Ключевые слова: проактивная защита, защита программного обеспечения, жизненный цикл программного обеспечения.

Основной отличительной особенностью подхода, связанного с проактивной защитой программного обеспечения (ПО), является то, что начало процесса защиты программ можно (и нужно) перенести на более ранние этапы их жизненного цикла, например на этапы, предшествующие этапу тестирования и испытаний ПО, тем самым увеличив общее время на внесение в программы защитных функций.

Здесь уместно процитировать слова Э.В. Дейкстра, одного из основоположников современной методологии программирования, сказанные им еще в 1972 г.[1]: «В настоящее время общепринятой техникой является составление программы, а затем ее тестирование. Однако тестирование программ может быть очень эффективным способом демонстрации наличия ошибок, но оно безнадежно неадекватно для доказательства их отсутствия... Не следует сначала

писать программу, а потом доказывать ее правильность, поскольку в этом случае требование найти доказательство только увеличит тяготы бедного программиста».

Эти слова как нельзя лучше подходят и к современной проблематике, связанной в данном случае с разработкой не столько правильных, сколько безопасных программ. Иными словами, ключом к созданию безопасного программного обеспечения является стремление защищаться от программных средств скрытого информационного воздействия (ПССИВ) с самого начала жизненного цикла программ, а не после факта их создания.

Модели и методы проактивной защиты программного обеспечения

Известные методы (классы методов) проактивной защиты ПО с привязкой к его жизненному циклу приведены на рис. 1. К ним относятся классы:

I. методов и инструментальных методик диагностического контроля инструментальных средств разработки ПО (трансляторов, компиляторов, отладчиков, CASE-средств)[2, 3, 4];

II. моделей и методов верификации программ, верификации моделей программ (см., например, сноску [5, 6]);

III. методов контроля проактивной безопасности ПО на этапах его автономных испытаний, комплексных испытаний, рекламационных доработок [7, 8];

IV. средств проактивной защиты на этапе подготовки ПО к функционированию: средств обновления ОС, антивирусных баз данных, баз данных сигнатур атак IDS/IPS-систем, систем активного аудита и т. п.;

V. моделей и методов проактивной защиты посредством методов Data Mining (см., например, сноску [9]) .

Из рис. 1 следует, что этапы (задачи) разработки функционально эквивалентных алгоритмов с введенными элементами защиты и их кодирования на конкретных языках программирования или кодирования в машинных кодах ранее практически не рассматривались в рамках единой технологии разработки защищенного ПО. Поэтому именно разработке моделей и методов защиты на этих этапах посвящена настоящая работа. Кроме того, в перечисленных выше классах методов проактивной защиты программ, как правило, не выдвигалось предположение о том, что при их разработке действует злоумышленник.

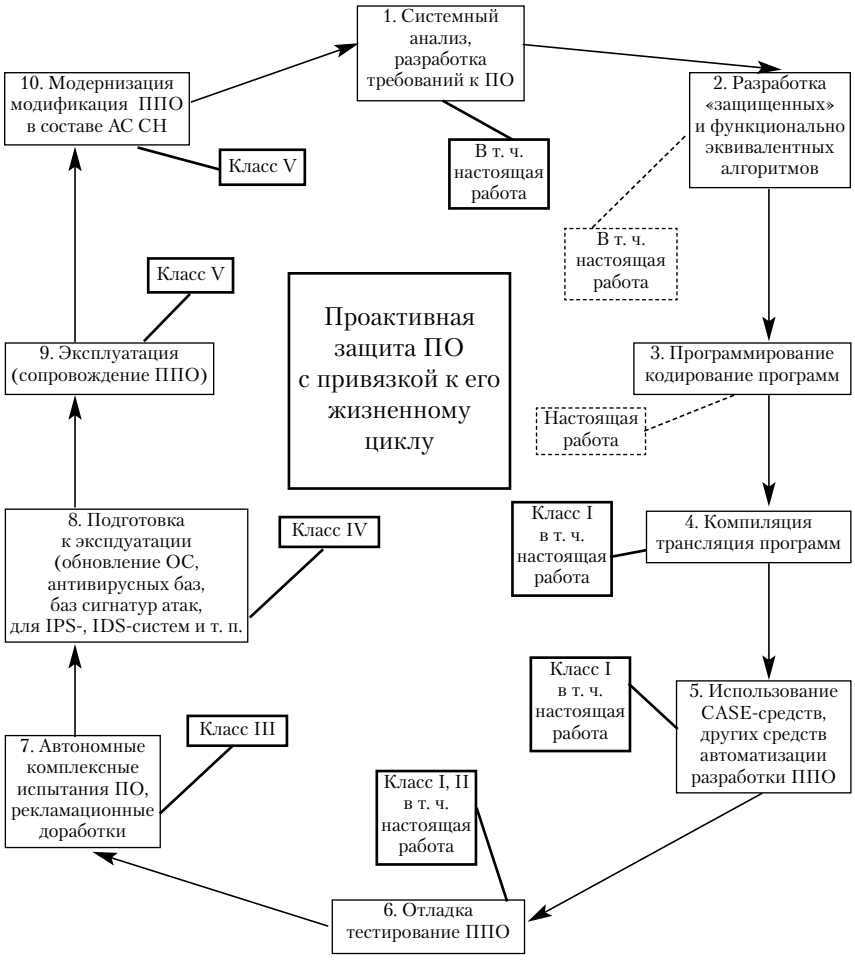


Рис. 1. Классы методов проактивной защиты ПО

Разработанные методы и решения по проактивной защите ПО на этапах системного анализа, разработки требований, математического и алгоритмического обеспечения, программирования (кодирования программ), их компиляции и отладки в совокупности с известными методами и решениями по проактивной защите на этапах тестирования и испытаний составляют полный методический базис структуры деятельности по проактивной защите ПО, что, в свою очередь, позволяет говорить о достаточности

и обоснованности набора лежащих в ее основе моделей и методов проактивной защиты ПО[10]. И, таким образом, разработанные методы и решения позволяют «теперь» охватить все этапы жизненного цикла ПО, предшествующие этапу его эксплуатации по назначению.

Анализ возможных решений показал[11, 12], что математических моделей и методов проактивной защиты от действий злоумышленника на ранних этапах жизненного цикла ПО скорее всего не может быть много (но они есть) ввиду как сложности формализации таких решений, так и сложности самих решений. А в результате анализа доступной литературы, проведенного в работе[13], можно было убедиться в том, что других методов проактивной защиты подобного рода пока нет (автору они не известны). Исключение, наверное, составляют методы построения доверенных сред на недоверенных элементах (см., например, сноску [14]) или методы обеспечения функциональной отказоустойчивости (см., например, сноску [15]). Но в этом случае скорее речь идет о системных (системотехнических), а не алгоритмических решениях, закладываемых в основу ПО для различных приложений.

Таким образом, в последнее время появилась насущная необходимость в создании новых технологий разработки ПО, изначально (с самого начала жизненного цикла) ориентированных на создание безопасных программных продуктов, когда на этапе его проектирования действуют (незначительная часть) злоумышленники.

В рамках указанного выше подхода автором настоящей работы исследовались три основных направления.

Первое направление основывается на так называемых протоколах конфиденциальных вычислений. Имеется n участников протокола или n процессоров вычислительной системы, соединенных сетью связи. Изначально каждому процессору известна своя часть некоторого входного значения x. Требуется вычислить $f(x)$, f – некоторая известная всем участникам вычислимая функция, таким образом, чтобы выполнились требования:

– корректности, когда значение $f(x)$ должно быть вычислено правильно, даже если некоторая ограниченная часть участников произвольным образом отклоняется от предписанных протоколом действий;

– конфиденциальность, когда в результате выполнения протокола ни один из участников не получает никакой дополнительной информации о начальных значениях других участников (кроме той, которая содержится в вычисленном значении функции).

Можно представить следующий сценарий использования этой модели для разработки безопасного программного обеспечения. Имеется некоторый процесс, для управления которым необходимо реализовать функциональность f. При этом последствия неправильной реализации таковы, что представляется целесообразным пойти на дополнительные затраты, связанные с созданием сети из n процессоров и распределенного алгоритма для реализации f. В системе имеется еще один абсолютно надежный участник, который имеет доступ к секретному значению x и имеет возможность выделить каждому процессору свою «долю» x. Название «Протоколы конфиденциальных вычислений» отражает тот факт, что требование конфиденциальности является основным, т. е. значение x не должно попасть в руки злоумышленника.

Данная модель позволяет единообразно трактовать как ошибки, возникающие, например, в результате сбоев технических средств, так и ошибки, возникающие за счет привнесения в вычислительный процесс ПССИВ. Следует отметить, что протоколы конфиденциальных вычислений относятся к протоколам, которые предназначены прежде всего для защиты процесса вычислений от действия «разумного» злоумышленника, т. е. от злоумышленника, который всегда выбирает наихудшую для нас стратегию.

Второе направление связано с разработкой так называемых самотестирующихся и самокорректирующихся программ. Пусть требуется разработать программу, вычисляющую функции f. Предположим, что реализация этой программы заказана исполнителю, который не пользуется полным доверием.

Самотестирующаяся программа разрабатывается как совокупность двух модулей. Первый из них вычисляет функцию f, второй модуль тестирует первый, подавая ему на вход некоторые значения $x_1, ..., x_k$ и сопоставляя полученный результат не с заранее вычисленными значениями функции f, а между собой. Чтобы этот подход имел право на существование, тестирующий модуль должен быть проще самого эффективного алгоритма вычисления функции f. Следует отметить также, что этот модуль должен быть надежным.

Подход, основанный на идее самотестирования, нашел свое развитие в так называемых самокорректирующихся программах. Такая программа также состоит из двух модулей, первый из которых вычисляет функцию f. Предполагается, что этот модуль может выдавать ошибочные (ложные) значения. Однако если это не происходит слишком часто, то второй, корректирующий, модуль,

выбирая некоторые значения x_l, ..., x_k и подавая их на вход первому модулю, скорректирует по полученным значениям все ошибки и вычислит правильное значение функции. На корректирующий модуль накладываются такие же требования эффективности, как и на тестирующий.

Задача разработки самотестирующихся и самокорректирующихся программ и их сочетаний представляет собой следующую задачу.

Пусть требуется разработать ПО, реализующее функциональность f. Реализация этого ПО заказана исполнителю, который не пользуется полным доверием. Однако последствия от негативной работы данного ПО таковы, что можно пойти на затраты, связанные с разработкой дополнительных тестирующих модулей, создание которых поручается специалисту, пользующемуся доверием. Таким образом, самотестирующееся ПО представляет собой набор программ, в которых в качестве подпрограмм используются целевые программы и который предназначен для их эффективного тестирования на предмет обнаружения ПССИВ.

К числу методов проактивной защиты следует также отнести методы разработки алгоритмического обеспечения создаваемого ППО с использованием защищенных модулей[16, 17, 18]. Необходимость разработки безопасного ПО с использованием защищенных модулей (ЗМ) возникает тогда, когда требуется обеспечить аутентификацию и целостность сложных программных комплексов, создаваемых большим коллективом разработчиков, среди которых могут быть злоумышленники. Такой модуль представляет собой защищенное от противника устройство, в котором в случае несанкционированного доступа к нему осуществляется физическое разрушение основных компонентов модуля: регистров процессора и ячеек памяти.

Чтобы достигнуть требуемого уровня защиты такого ПО, работа с конфиденциальными параметрами, вводимыми в ЗМ, поручается доверенным разработчикам. Задачу разработки безопасного ПО с использованием ЗМ при этом предлагается решать путем разработки программно-аппаратного пакета, состоящего из ЗМ, защищаемой программы и протоколов взаимодействия между ними.

Эти направления защиты могут быть положены в основу деятельности по проактивной защите ПО, при этом изначально предполагается, что:

– один или несколько участников проекта являются (или, по крайней мере, могут быть) злоумышленниками;

– в процессе разработки и эксплуатации злоумышленник может вносить в программы ПССИВ;

– средства вычислительной техники, на которых выполняются программы, не свободны от аппаратных закладок.

Таким образом, научно-практические основы организации деятельности по обеспечению проактивной защиты программного обеспечения представляют собой совокупность организационно-технических решений, моделей и методов, рассматриваемых в рамках данной деятельности, которые позволяют выполнить следующий сценарий разработки ПО. Имеется некоторый процесс, для управления которым необходимо реализовать функциональность f. При этом последствия неправильной реализации f таковы, что представляется целесообразным пойти на дополнительные затраты, связанные с созданием сети из n процессоров и распределенного алгоритма для реализации f, разработкой дополнительных оракульных программ с вызовом целевой программы вычисления f, введением в схемы вычисления f защищенных модулей.

Тогда схемы и протоколы защиты, реализующие предлагаемые методы, могут позволить получить корректную функциональность f, даже если среди разработчиков ПО присутствуют злоумышленники, способные внедрять ПССИВ.

Заключение

Разработка современных моделей и методов проактивной защиты ПО включает:

• создание моделей и методов проактивной защиты программного обеспечения, используемых на этапах проектирования, разработки и испытания программных комплексов;

• создание моделей, методов и инженерных методик функционирования распределенного программного обеспечения в виде сетей взаимодействующих процессов и окружения:

• поддержка ранних этапов анализа и проектирования спецификаций, оптимального выбора проектных решений на основе методик и метрик оценки и прогнозирования трудоемкости, ресурсоемкости, сложности и безопасности вариантов проектирования ПО;

• контроль корректности реализации и верификации протоколов взаимодействующих процессов, выбора критериев оценки эффективности и защищенности распределенного ПО, их реализующих.

В настоящей работе сделана попытка выявить необходимость разработки новых моделей и методов проактивной защиты программного обеспечения, являющегося центральным информационно-активным звеном современных автоматизированных систем. При этом применение новых подходов, алгоритмов, схем и протоколов защиты позволяет перенести процесс внесения в ПО защитных функций на более ранние этапы его жизненного цикла.

Примечания

[1] См.: *Дейкстра Э.В.* Смиренный программист // Лекции лауреатов премии Тьюринга за первые 20 лет. 1966–1985. М.: Мир, 1993.

[2] См.: *Ефимов А.И.* Проблема технологической безопасности программного обеспечения систем вооружения // Безопасность информационных технологий. 1994. № 3–4. С. 22–33.

[3] См.: *Ефимов А.И., Пальчун Б.П., Ухлинов Л.М.* Методика построения тестов проверки технологической безопасности инструментальных средств автоматизации программирования на основе их функциональных диаграмм // Вопросы защиты информации. 1995. № 3 (30). С. 52–54.

[4] См.: Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. [Электронный ресурс] URL: http://www.fstec.ru/_docs/doc_3_3_010.htm (дата обращения: 06.02.2012).

[5] См.: *Пучков Ф.М., Шапченко К.А., Андреев О.О.* К созданию автоматизированных средств верификации программного кода // Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 окт. 2004 г. М.: МЦНМО, 2004. С. 347–359.

[6] См.: *Кларк Э.М., Грамберг О., Пелед Д.* Верификация моделей программ: Model Checking. М.: МЦНМО, 2002.

[7] См.: *Ефимов А.И.* Указ. соч.

[8] См.: *Ефимов А.И., Ухлинов Л.М.* Методика расчета вероятности наличия дефектов диверсионного типа на этапе испытаний программного обеспечения вычислительных задач // Вопросы защиты информации. 1995. № 3 (30). С. 86–88.

[9] См.: *Комашинский Д.В., Котенко И.В.* Исследование проактивных механизмов обнаружения вредоносного программного обеспечения на базе методов Data Mining // Математика и безопасность информационных технологий. Материалы конференции в МГУ 30–31 окт. 2008 г. Т. 2. М.: МЦНМО, 2009. С. 226–231.

[10] См.: *Казарин О.В.* Методология защиты программного обеспечения. М.: МЦНМО, 2009. 464 с.

[11] Там же.

[12] См.: *Казарин О.В., Скиба Л.М.* Парадигма проактивной безопасности компьютерных систем // Защита информации. INSIDE. 2009. № 5. С. 2–9; № 6. С. 2–7.

[13] См.: Там же.

[14] См.: *Грушо А.А., Грушо Н.А., Тимонина Е.Е.* Методы защиты информации от атак с помощью скрытых каналов и враждебных программно-аппаратных агентов в распределенных системах // Вестник РГГУ. 2009. № 10/09. С. 33–45. Сер. «Информатика. Защита информации. Математика».

[15] См.: *Тарасов А.А.* Функциональная отказоустойчивость систем обработки информации. М.: МИНИТ ФСБ России, 2009. 184 с.

[16] См.: *Варновский Н.П.* Стойкость электронной подписи в модели с защищенным модулем // Дискретная математика. 2008. Т. 20. Выпуск 3. С. 147–159.

[17] См.: *Казарин О.В., Ухлинов Л.М.* Интеллектуальные средства обеспечения безопасности данных в информационно-вычислительных сетях // Вестник РОИВТ. 1994. № 3. С. 35–46.

[18] См.: *Varnovsky N.* Provable security of digital signature in the tamper-proof model. [Электронный ресурс] URL: http://www.eprint.iacr.org/ 2008/ (дата обращения: 06.02.2012).

А.Н. Приезжая

АВТОМАТИЗИРОВАННОЕ ФОРМИРОВАНИЕ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Процесс разработки модели угроз требует трудоемкого анализа защищаемого. В данной статье предлагается технология, основанная на автоматизированном преобразовании моделей, которая позволяет одновременно разрабатывать несколько представлений объекта, включая текстовое описание, и в автоматизированном режиме строить на их основе модели угроз и нарушителя.

Ключевые слова: модель, персональные данные, преобразование моделей, модель объекта, модель угроз.

В настоящее время мы живем в информационном обществе. Что это означает? Это означает, что мы зависим от информации, в частности, для нормального функционирования современного общества необходим оперативный доступ к достоверной информации наряду с необходимостью обеспечения конфиденциальности чувствительной информации. При этом для хранения и обработки информации используются уязвимые технологии (в том числе распределенные информационные системы с подключением к сетям связи общего пользования). Иными словами, перед обществом и государством, бизнес-организациями стоит задача нахождения компромисса между потребностями в доступе к информации и необходимостью ее защиты. Существуют различные подходы к созданию защищенных информационных систем: на основе анализа угроз и рисков[1], на основе анализа структуры системы[2] и др. При этом при определении требований к защите информации без учета угроз ценные активы организации могут

получить недостаточный уровень защиты, а расходы на защиту малоценных активов станут неоправданно высокими.

Для определения необходимых и достаточных мер защиты информационных систем формируется модель угроз безопасности информационной системы. Модель угроз предназначена для выявления актуальных для конкретной информационной системы угроз безопасности и формирования на ее основе требований к защите рассматриваемой информационной системы. Выявление актуальных угроз безопасности – процесс трудоемкий и сложный, требующий работы квалифицированного эксперта, что определяется следующими основными факторами: возрастающей сложностью современных информационных систем и постоянно изменяющимся множеством угроз.

Таким образом, для упрощения и удешевления процесса формирования модели угроз необходимо создать инструмент поддержки анализа. В данной статье рассматривается подход к созданию такого инструмента на примере разработки модели угроз и нарушителя для информационной системы персональных данных: в первой части статьи рассматривается общий принцип формирования модели угроз, в последующих частях – формирование отдельных составляющих данного документа, в заключительной части рассматриваются возможности применения данного инструмента.

Формирование модели угроз и модели нарушителя информационной системы персональных данных должно осуществляться в соответствии с требованиями нормативно-методических документов в области защиты информации. В соответствии с анализом[3] нормативно-методических документов ФСТЭК и ФСБ России в рамках разработки модели угроз безопасности персональных данных должны быть разработаны следующие модели:

– модель нарушителя, позволяющая провести классификацию системы и выбрать необходимый уровень криптографической защиты в соответствии с руководящими документами ФСБ России;

– модель угроз, включающая перечень актуальных угроз (способов реализации), позволяющий определить требуемый уровень защиты автоматизированной системы от НСД и утечки по техническим каналам в соответствии с руководящими документами ФСТЭК России.

Как показал анализ нормативно-методических документов-регуляторов, для построения модели угроз необходимо определить объекты воздействия (защищаемые ресурсы), цели атак (или воз-

можный несанкционированный доступ) и определить возможные способы доступа (каналы атак) и их актуальность. При этом для определения перечня возможных способов доступа необходимо провести анализ уязвимостей системы и возможностей нарушителя.

Анализ объекта может быть проведен с применением различных методик. Одной из возможных методик анализа является моделирование, которое позволяет получить обозримое и полное представление системы с требуемым уровнем детализации, кроме того, формализованная модель объекта может быть использована для автоматизированного получения модели угроз и в дальнейшем для построения модели защиты. Модель угроз может быть построена различными способами. В данной статье рассматривается построение модели угроз с использованием ряда базовых и прикладных моделей, характеризующих различные аспекты объекта защиты.

Базовые модели используются для генерации прикладных моделей и содержат:

– перечень возможных угроз безопасности с указанием необходимых для их реализации средств и знаний, последствий их реализации;

– базовые модели нарушителей с указанием категорий лиц потенциальных нарушителей и их возможностей;

– методику оценки ущерба при нарушении состояния защищенности элемента объекта.

Прикладные модели описывают конкретный объект защиты, в рамках формирования модели угроз создаются следующие прикладные модели:

– модель объекта защиты;

– модель потенциальных точек воздействия;

– модель нарушителя;

– модель угроз.

Формирование модели конкретного объекта защиты осуществляется путем задания свойств элементов модели объекта. Модель объекта должна быть построена максимально полной, с различными представлениями объекта и различными уровнями детализации, так как информация, которая покажется избыточной на одном этапе, может быть использована на следующих стадиях создания системы, например, данные об используемых протоколах не нужны для определения принципов построения системы защиты, но могут оказать влияние на выбор технических средств защиты.

Целью защиты информации является сохранение состояния защищенности информации, при этом доступ к информации, как правило, осуществляется через некоторого посредника. В частности, для информации в качестве таких посредников могут выступать:

– программное обеспечение, обеспечивающее ввод, обработку и хранение информации;

– ОТСС, задействованные для передачи, обработки и хранения информации;

– ВТСС, связанные с ОТСС (в том числе расположенные в одном помещении);

– персонал, работающий информацией и/или СВТ;

– помещение, в котором происходят ввод, обработка и хранение информации.

Иными словами, для обеспечения состояния защищенности информации необходимо выявить и обеспечить безопасность всех ресурсов, представляющих ценность для организации, а также тех ресурсов, через которые возможен доступ, т. е. должен быть определен перечень защищаемых ресурсов, при этом должны быть определены последствия нарушения состояния защищенности информации (ресурсов). Состояние защищенности информации может быть определено через следующие свойства:

– конфиденциальность (защищенность информации от несанкционированного раскрытия информации об объекте);

– целостность (защищенность информации от несанкционированной модификации, уничтожения);

– доступность (обеспечение своевременного санкционированного получения доступа к информации);

– подконтрольность – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта; обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены индивидуально по отношению к субъекту;

– достоверность – свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам, как пользователи, процессы, системы и информация; идентичность объекта к тому, что заявлено.

Соответственно для каждого ресурса в модели объекта определяются защищаемые свойства и последствия их нарушения (ущерб). При формировании модели объекта необходимо учитывать, что объект защиты содержит разнородные защищаемые ресурсы, в частности:

• защищаемую информацию; причем в рамках объекта защиты (ОЗ) могут существовать различные типы информации, например:
  – информация, представляющая собой ПДн (Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);
  – служебная информация и информация ограниченного распространения, составляющая служебную тайну;
  – информация, используемая для идентификации и аутентификации пользователей ОЗ;
  – ключевая информация средств криптографической защиты;
  – информация журналов регистрации событий;
• сведения о средствах и системе защиты информации ОЗ;
• СВТ и их компоненты, в частности:
  – средства хранения и обработки информации ОЗ;
  – активное сетевое оборудование ОЗ;
  – АРМ пользователей;
  – средства защиты;
• общее и специальное программное обеспечение ОЗ:
  – операционные системы СВТ ОЗ;
  – общесистемное программное обеспечение ОЗ;
  – специальное программное обеспечение ОЗ;
• сведения о технологическом устройстве ОЗ:
  – логические схемы функционирования ОЗ;
  – топология и сетевая архитектура ОЗ.

Кроме того, возможности по доступу нарушителя к защищаемым ресурсам зависят от структуры объекта, используемых технических средств, характера информационных взаимодействий между компонентами системы, а также принятых организационно-режимных и технических мер защиты и особенностей размещения объекта защиты. Все значимые для обеспечения безопасности характеристики объекта описываются в его модели.

Основными задачами формирования модели объекта защиты являются:

– описание структуры системы;

– идентификация защищаемых ресурсов ОЗ и оценка ущерба, который может быть нанесен при нарушении характеристик безопасности ЗР;

– выявление потенциальных точек воздействия – элементов системы, которые могут быть использованы для нарушения характеристик безопасности ЗР.

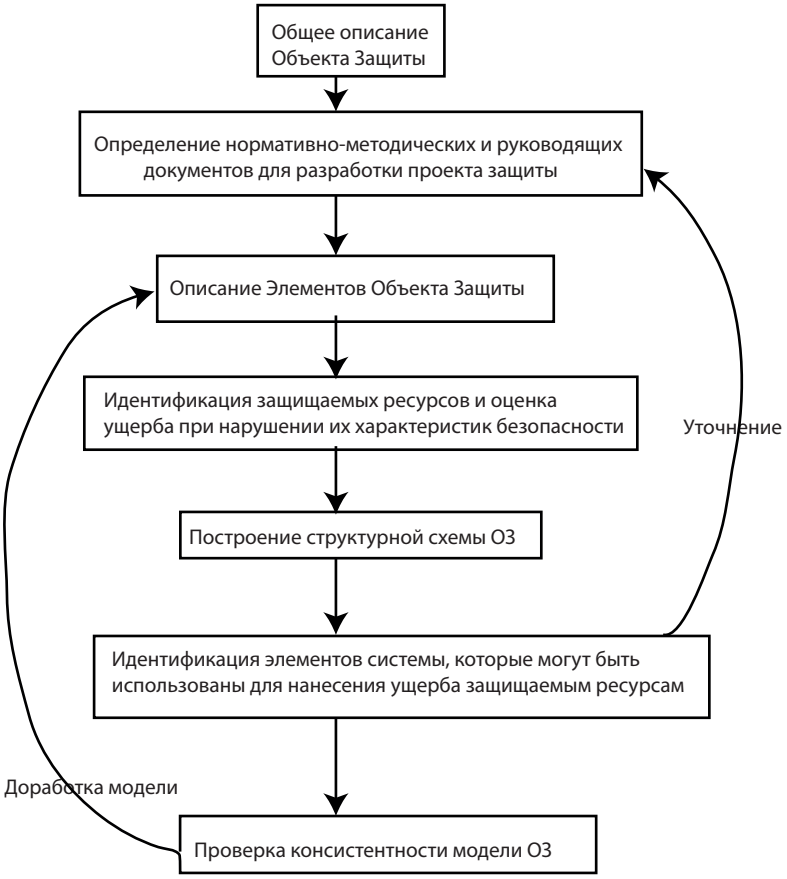


Рис. 1. Алгоритм формирования модели объекта

Алгоритм формирования модели объекта приведен на рис. 1. Структура ОЗ описывается прикладной моделью «Объект защиты». При этом система представляется как совокупность элементов и связей между ними. Структура и правила построения модели объекта защиты приведены на рис. 2.

Модель ОЗ содержит:

– информацию в форме, пригодной для дальнейшей автоматизированной обработки;

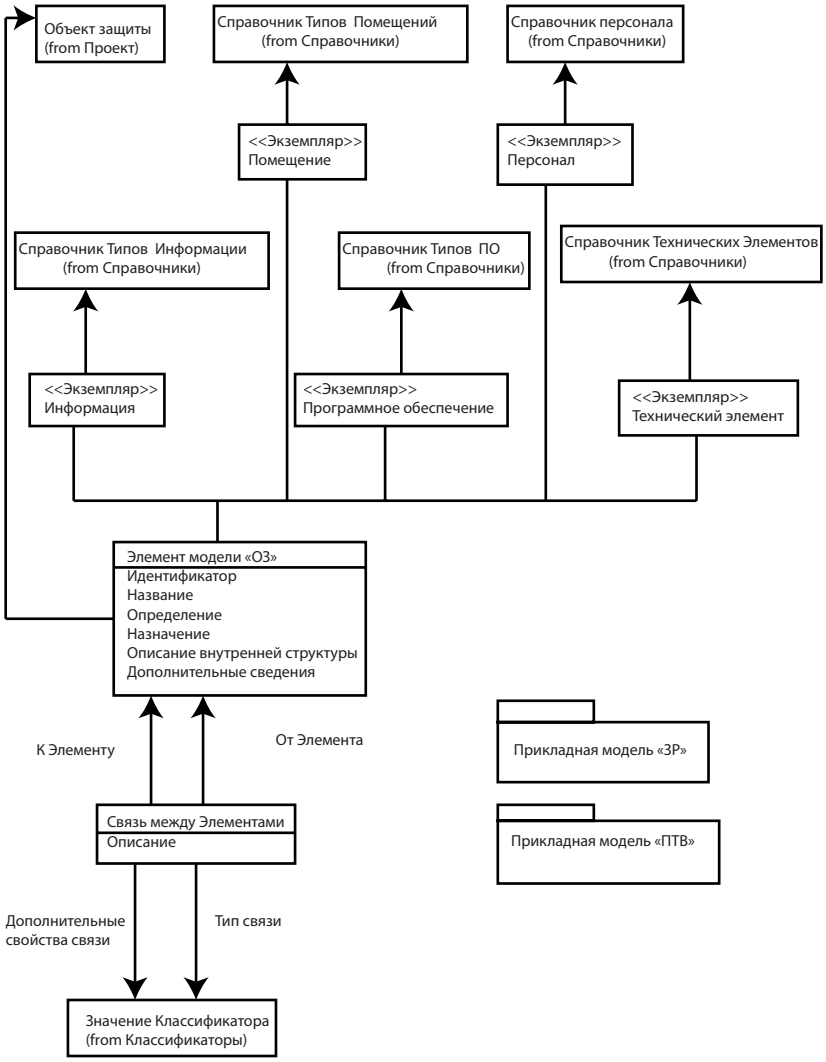


Рис. 2. Структура модели ОЗ

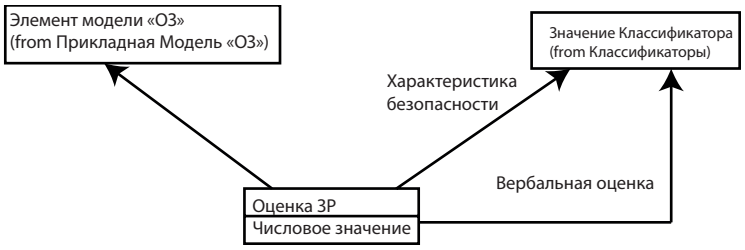


Рис. 3. Оценка защищаемых ресурсов

– детальную информацию в форме, пригодной для проведения экспертного анализа и использования в проектных документах.

Для последующей автоматической обработки каждый элемент модели типизируется. Определяются класс элемента (информация; программное обеспечение; технические элементы; помещения; персонал и пользователи ОЗ) и тип элемента с использованием соответствующего справочника.

Для связи определяются:

элементы системы, которые она связывает;

тип связи – значение, выбираемое из системного классификатора «Тип связи» (для выбора доступны только те значения, которые применимы для данных элементов системы с учетом их класса);

– описание связи (необязательный параметр. Содержит важную для экспертного анализа информацию. Использование в проектных документах не предполагается);

– дополнительное свойство связи (необязательный параметр).

Идентификация защищаемых ресурсов происходит автоматически (рис. 3). Элемент системы считается защищаемым ресурсом, если в соответствии с базовой моделью для элемента данного типа задана ненулевая шкала ущерба при нарушении хотя бы одного свойства. Эксперт должен произвести вербальную оценку всех элементов системы, идентифицированных как ЗР, с использованием шкалы, рекомендованной для данного типа элемента в базовой модели «Методика оценки ущерба при нарушении характеристик безопасности».

По результатам вербальной оценки формируется числовое значение, используемое для оценки интегрального ущерба: числовой эквивалент вербальной оценки умножается на весовой коэффициент, заданный в базовой модели.

Элементы системы, получившие по результатам экспертной оценки нулевую оценку ущерба при нарушении всех характеристик безопасности, в дальнейшем не рассматриваются как защищаемый ресурс системы.

При определении возможных атак необходимо учитывать, что атака, реализующая ту или иную угрозу, может происходить в несколько этапов, т. е. помимо защищаемых ресурсов должны быть определены потенциальные точки воздействия – элементы ОЗ, посредством которых может быть проведена атака на защищаемую информацию. Элемент системы является потенциальной точкой воздействия (ПТВ), если существует хотя бы одна атака, гарантирующая нанесение ущерба всем связанным ресурсам.

Выявление потенциальных точек воздействия и расчет коэффициентов уязвимости происходят автоматически с использованием базовой модели «Потенциальные точки воздействия» (модель ПТВ) и могут быть скорректированы экспертом в ручном режиме. Модель ПТВ описывает относительную эффективность воздействия на ЗР путем атаки различных элементов системы, рассматриваемых как ПТВ.

Оценки проводятся с использованием вербальной шкалы (с числовым эквивалентом в процентах).

Модель ПТВ имеет два подтипа:

– точную модель, предназначенную для использования в детально проработанной модели ОЗ;

– модель унаследованного ущерба, предназначенную для использования с моделями ОЗ верхнего уровня.

В детальной модели прорабатываются все связи между элементами системы. В этой модели предполагается, что нарушение конфиденциальности информации возможно только при воздействии на СУБД.

В модели унаследованного ущерба предполагается, что элементы, связанные (прямо или опосредовано) с СУБД – сервер, серверная, администратор, тоже хранят информацию, а атака на эти элементы может нанести такой же ущерб, как и атака на СУБД.

Правила интерпретации модели.

1. Если для какого-либо сочетания значений из справочников ЗР и ПТВ не заданы коэффициенты уязвимости, то считается, что для данного сочетания должны использоваться (наследоваться) коэффициенты уязвимости ближайших (по иерархии) типов ЗР и ПТВ, для которых данные ЗР и ПТВ являются подтипами, а коэффициенты уязвимости заданы.

2. Если такого сочетания нет, считается что тип элемента из справочников ПТВ не может использоваться для нанесения ущерба ЗР данного типа.

Алгоритм идентификации ПТВ следующий:

– формируется список Э1 элементов системы, идентифицированных как ЗР;

– для каждого элемента списка Э1 формируется список S1 связей, исходящих от этого элемента системы;

– для каждой связи из списка S1 определяется ее тип и тип (второго) связанного элемента ОЗ. Данный элемент системы рассматривается как кандидат на роль ПТВ.

Если в базовой модели ПТВ определены ненулевые коэффициенты уязвимости (для точной модели и/или модели унаследованного ущерба), то кандидат идентифицируется как ПТВ и заносится в список Э2 (если он не содержится в списке S1), а коэффициенты записываются в модели ОЗ.

После завершения просмотра S1 формируется список связей для следующего элемента списка Э1 и процедура анализа связей повторяется. После просмотра всех элементов списка Э1 проверяется список Э2. Если в этом списке есть хотя бы один элемент, то процесс проверки повторяется с элементами списка Э2, в противном случае считается, что все ПТВ идентифицированы.

В процессе анализа списка автоматически идентифицированных ПТВ эксперт может сформировать свою (в том числе нулевую) оценку коэффициента уязвимости с использованием вербальной шкалы. Элементы системы, получившие по результатам автоматизированной или экспертной оценки нулевую оценку коэффициентов уязвимости при нарушении всех характеристик безопасности всех защищаемых ресурсов системы, в дальнейшем не рассматриваются как ПТВ.

Одним из этапов построения модели «Объект защиты» в процессе информационного обследования является инвентаризация ЗР и оценка ущерба, который может быть нанесен при нарушении характеристик безопасности ЗР. Эти оценки проводятся с использованием вербальной шкалы.

При построении моделей ОЗ и модели угроз производится расчет интегрального ущерба, наносимого всем защищаемым ресурсам. При этом происходит переход от вербальных оценок к их числовому эквиваленту, определенному в соответствующем классификаторе и суммирование полученных значений с использованием весовых коэффициентов, заданных в модели.

Методика оценки может быть задана для следующих свойств: конфиденциальность; целостность; доступность; подконтрольность; достоверность.

Перечень свойств может быть расширен при необходимости путем добавления новых в классификатор и описания соответствующих им методик оценки.

Правила интерпретации модели.

Если для какого-либо значения, описывающего защищаемые ресурсы (типов информации, типов ПО, типов технических элементов), не задана методика оценки, то считается, что для данного ЗР должна использоваться (наследоваться) методика ближайшего (по иерархии) типа ресурса, для которого данный ресурс является подтипом, а методика оценки задана.

Если какой-либо тип верхнего уровня ресурсов верхнего уровня не является защищаемым ресурсом, для него должна быть указана методика нулевого ущерба.

Если для какого-либо типа ресурса верхнего уровня не задана никакая методика, то к нему (и его подтипам) должна применяться методика максимального ущерба.

Следующим шагом определения перечня актуальных угроз является построение модели нарушителя. Описание возможностей нарушителя безопасности данного объекта защиты строится на основании базовой модели «Возможности нарушителя». Данная модель описывает максимальные возможности для типов нарушителей. Алгоритм формирования модели нарушителя приведен на рис. 4.

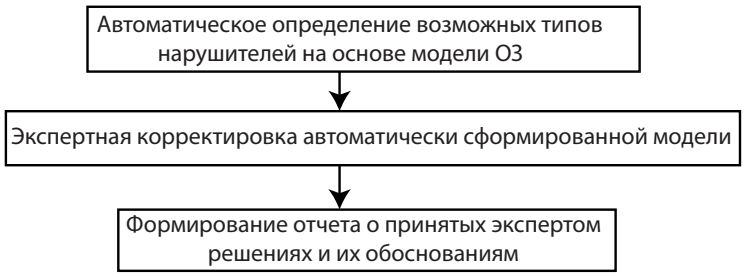


Рис. 4. Алгоритм формирования модели нарушителя

Возможности нарушителя определяются двумя составляющими:

– технической вооруженностью (доступными техническими средствами проведения атак);

– информационной вооруженностью (знания о способах и методах проведения атак, сведения об особенностях объекта защиты, включая сведения о системе защиты информации, уровень подготовки).

Так, техническая вооруженность включает в себя возможность доступа к штатным средствам АСЗИ, доступным в свободной продаже, или специально разработанным средствам проведения атак (например, анализа сетевого трафика, перехвата информации по каналам ПЭМИН), средствам активации аппаратных закладных устройств и т. п. При этом каждое средство проведения атаки связано с каналом атаки, для которого оно применимо.

Информационная и техническая вооруженность определяет перечень возможных каналов и способов проведения атак для данного типа нарушителя.

Тип нарушителя (и его базовые возможности) определяется исходя из категории лиц – потенциальных нарушителей, в качестве потенциальных нарушителей рассматриваются хакеры, хулиганствующие элементы, обиженные сотрудники, криминальные структуры и др. Данным категориям сопоставляются шесть типов нарушителей, характеризующихся определенными возможностями. Базовая модель «Возможности нарушителя» описывает максимальные возможности для типов нарушителей.

Правила интерпретации модели.

Подтип типа нарушителя наследует все возможности типов нарушителя, расположенных выше по иерархии.

Модель является обучаемой (адаптивной) при добавлении новой возможности в прикладной модели, такая же возможность добавляется соответствующему типу нарушителя в базовой модели с областью применения «Проект».

Возможности нарушителя ограничиваются применяемыми на объекте защиты организационными и техническими мерами, в частности, возможности внутреннего нарушителя ограничиваются принятыми правилами пропускного и объектового режимов. Данные о принятых ограничениях хранятся в прикладной модели объекта.

Применительно к каждому конкретному проекту перечень возможностей нарушителя можно дополнять или сокращать, при этом контролируется полнота описания возможности, так как, в соответствии с принятыми правилами формирования моделей, ограничения на возможности нарушителя должны быть мотивированы. Сведения о возможностях нарушителя информационной

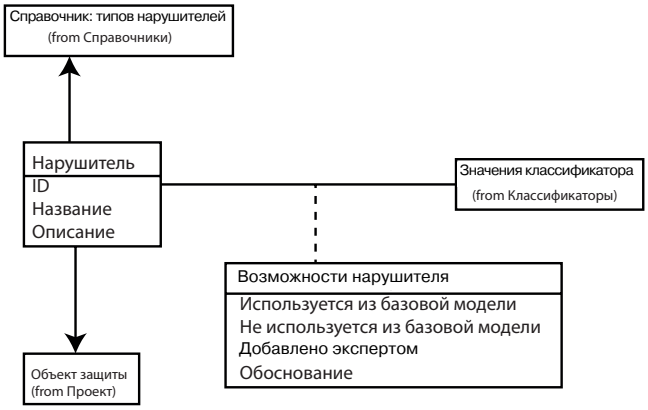


Рис. 5. Прикладная модель «Типы нарушителей и их возможности»

безопасности данного объекта защиты хранятся в прикладной модели «Типы нарушителя и их возможности».

Прикладная модель «Типы нарушителей и их возможности» (рис. 5) строится на основе базовой модели «Возможности нарушителя» и содержит:

– информацию в форме, пригодной для дальнейшей автоматизированной обработки;

– детальную информацию в форме, пригодной для проведения экспертного анализа и использования в проектных документах.

При последующей автоматической обработке для каждого нарушителя должен быть определен его тип с использованием справочника типов нарушителей (базовой модели нарушителя). Таким образом, возможности (знания и средства), каналы атаки и возможные способы доступа нарушителя определяются автоматически на основании базовой модели нарушителя и модели объекта защиты (структуры системы и перечня защищаемых ресурсов; ограничений на возможности нарушителя).

На основании модели нарушителя, содержащей возможные каналы атаки и способы доступа нарушителя, формируется модель угроз, содержащая перечень актуальных угроз безопасности информации.

Логическая схема алгоритма формирования модели угроз приведена на рис. 6.

Перечень возможных угроз определяется автоматически на основании прикладных моделей нарушителя, объекта защиты,

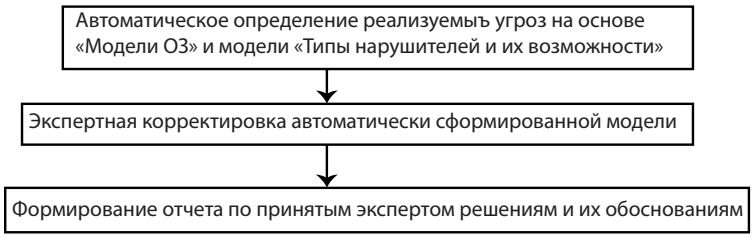


Рис. 6. Алгоритм формирования модели угроз

а также базовых моделей потенциальных точек воздействия, сценариев атак.

После определения перечня возможных угроз безопасности объекта защиты необходимо провести оценку актуальности угроз. Методика оценки актуальности угрозы зависит от вида информации (персональные данные, коммерческая тайна, иная информация конфиденциального характера, защищаемая информация).

Алгоритм оценки реализуемости угроз работает следующим образом.

1) Формируется список У1 всех угроз, определенных в справочнике «Типы угроз».

2) Для каждого элемента списка У1 в соответствии с базовой моделью «Сценарии атак» формируется список А1 атак, которые могут реализовать данную угрозу. Структура модели приведена на рис. 7.

Модель описывает: условия успешного проникновения (первого воздействия на элементы ОЗ); условия развития атаки (распространение от одного элемента ОЗ к другому); последствия успешного проведения атаки на элементы ОЗ.

Для каждой атаки из списка А1 проверяется возможность ее реализации. Условия успешного воздействия зависят от:

– типа ПТВ (как правило, условие описывается для элементов верхнего уровня, использование подтипов оправдано лишь тогда, когда последний обладает уязвимостями, отсутствующими у элемента верхнего уровня);

– свойств конкретного экземпляра ПТВ (элемента прикладной модели);

– возможностей нарушителя;

– канала доступа.

Условия успешного развития атаки зависят от:

– типа ПТВ, из которой происходит распространение атаки;

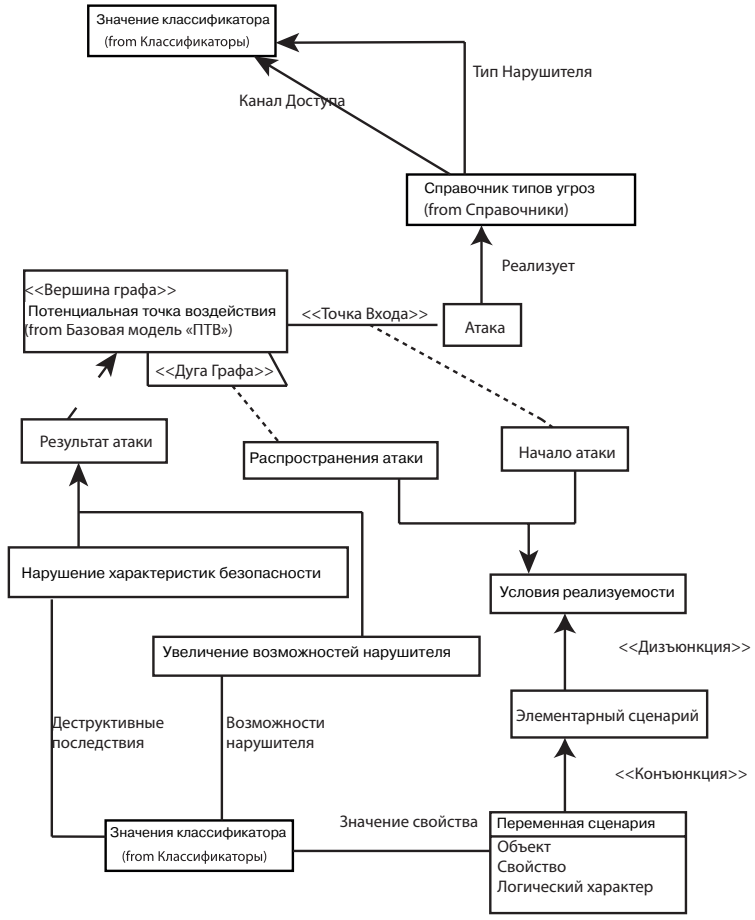


Рис. 7. Структура модели «Сценарии атак»

– свойств конкретного экземпляра ПТВ (элемента прикладной модели), из которого происходит распространение атаки;

– типа ПТВ, на который происходит распространение атаки;

– свойств конкретного экземпляра ПТВ (элемента прикладной модели), на который происходит распространение атаки;

– типа связи между ПТВ и, возможно, других свойств этой связи;

– канала доступа;

– возможностей нарушителя.

Условия описываются в дизъюнктивной нормальной форме (дизъюнкция элементарных сценариев). Условие реализации элементарного сценария описывается как конъюнкция переменных сценария.

Переменная сценария является свойством одного из объектов:

– ПТВ, на которую направлено воздействие;

– ПТВ, из которой происходит распространение;

– связи между ПТВ в прикладной модели ОЗ;

– нарушителя;

– значение свойства должно принадлежать одному из классификаторов.

Переменная сценария есть результат проверки одного из условий:

– «Равно» – значение свойства равно заданному значению из классификаторов;

– «Не равно» – значение свойства не равно заданному значению из классификаторов;

– «Входит» – значение свойства принадлежит заданному подмножеству значений из классификаторов;

– «Не входит» – значение свойства не принадлежит заданному подмножеству значений из классификаторов.

Успешное проведение (распространение) атаки на элемент ОЗ может приводить к таким последствиям, как нарушение характеристик безопасности (характеризуется одним или несколькими деструктивными последствиями); увеличение возможностей нарушителя.

Также на данном шаге алгоритма для каждой реализованной атаки в рабочих массивах алгоритма фиксируется:

– интегральный ущерб, который наносит данная атака ОЗ;

– возможности нарушителя, использованные в атаке;

– новые возможности, которые получил нарушитель в результате реализации данной атаки;

– деструктивные последствия атаки (в вербальной форме);

– элементы системы, которые использовались в качестве точки входа;

– элементы системы, на которые распространилась атака;

– ЗР, характеристики которых были нарушены в результате атаки;

– детальная информация о развитии атаки в виде текста (протокола развития атаки).

3) Если для угрозы есть хотя бы одна реализуемая атака, угроза заносится в прикладную модель угроз. При этом в модели угроз фиксируется следующая информация:

– максимальный ущерб, который наносит данная атака ОЗ (максимум по реализуемым атакам);

– возможности нарушителя, использованные в успешных атаках (объединение по реализуемым атакам);

– новые возможности, которые получил нарушитель в результате реализации данной угрозы (объединение по реализуемым атакам);

– деструктивные последствия угрозы (объединение по реализуемым атакам);

– элементы ОЗ, которые использовались в качестве точки входа угрозы (объединение по реализуемым атакам);

– элементы системы, на которые распространилась угроза (объединение по реализуемым атакам);

– ЗР, характеристики которых были нарушены в результате реализации угрозы (объединение по реализуемым атакам);

– детальная информация о способах реализации угрозы (объединение протоколов по реализуемым атакам).

4) После просмотра все угроз формируется список дополнительных возможностей нарушителей. Если список не пустой, то:

– нарушителям добавляются возможности, которые они приобрели в результате успешно проведенных атак;

– проводится повторная оценка реализуемости угроз с учетом изменившихся возможностей нарушителей.

5) После завершения второй итерации сравниваются списки дополнительных возможностей нарушителей, полученные на этой и предыдущей итерации. Если списки не совпадают, то выполняется еще одна итерация.

6) Процесс завершается, если списки дополнительных возможностей нарушителя, полученные в двух последовательных итерациях, совпадают.

Использование данного подхода предполагает, что любая модель может быть обоснованно скорректирована экспертом и все полученные прикладные модели могут быть представлены в текстовом виде с использованием генератора документов по шаблону. Предложенный в данной статье метод разработки модели угроз может быть использован вне зависимости от информации, обрабатываемой в информационной системе (персональные данные, коммерческая тайна, государственная тайна, иные сведения огра-

ниченного доступа, общедоступная информация), при этом для каждого вида информации необходимо создание (уточнение) методики оценки.

На основании полученных моделей может быть также произведена автоматизированная разработка системы защиты информации.

Примечания

[1] См.: *Приезжая А.Н.* Автоматизированная разработка защищенной информационной системы // Вестник РГГУ. 2010. № 12/10. С. 221–238. Сер. «Информатика. Защита информации. Математика»; Там же.

[2] См.: *Peterson M.J., Bowles J.B., Eastman C.M.* UMLpac: An Approach for Integrating Security into UML Class Design, 6 с. [Электронный ресурс] URL: http://www.cse.sc.edu/~yoncek/REU/PetersonPaper.pdf (дата обращения: 06.02.2012).

[3] См.: *Приезжая А.Н.* Технологии встраивания функций безопасности в бизнес-процессы // Вестник РГГУ. 2009. № 10/09. С. 71–84. Сер. «Информатика. Защита информации. Математика».

Abstracts

D.A. Larin

DATA PROTECTION AND CRYPTANALYSIS IN THE USSR DURING THE BATTLE OF STALINGRAD

July 17, 2012 marks the completion of 70 years since one of the greatest battles ever fought – the Battle of Stalingrad. This battle was the turning point of World War II, which ended with the complete defeat of Nazi groupings and their allies. Important role in the victory at Stalingrad was played by the Soviet cryptographers. Ciphers officers and cryptograph developers, cryptographic service and signal corps ensured the Soviet lines safety. Radio intelligence officers and decryptors successfully intercepted and deciphered the cryptogram of Nazi Germany and its European allies.

Keywords: cryptography, encryption, decryption, cipher, encoder, communication, Stalingrad.

S.V. Zapechnikov

ABOUT THE CRYPTOGRAPHY HISTORY. THE LEONARDO EULER'S CONTRIBUTION IN FORMATION OF MATHEMATICAL BASIS FOR MODERN CRYPTOLOGY

The article constitutes series of historic studies and at the same time an attempt to analyze scientifically a brilliant stage for Russian and world mathematics. This stage is associated with Leonardo Euler who was the great scientist in mathematics, mechanics and physics. It expounds the role of L. Euler in foundation of number theory, as well as ways of using his achivements by modern scientists and observes some historical aspects of creating the Russian educational system in mathematics. Special attention is paid to the importance of Euler's works for modern asymmetric cryptology (open key cryptology) and for the theory of cryptology protocols.

Keywords: cryptography history, number theory, prime numbers, computationally hard problems, mathematical education, modern cryptology.

Y.S. Chemerkin

PRACTICAL APPLICATION OF CLOUD SOLUTIONS FOR CONFIDENTIAL DATA PROCESSING

Nowadays Cloud solutions are the most promising kind of IT technologies due to its flexibility, efficiency and economic benefits, resulting in what is still a place for debates on the lack of protection from these technologies. Therefore one has to research the existing problems and to define their impact to be able to investigate possible ways of solving problems and reducing risks while the cloud computing implementation.

This paper considers the legal documents issues related to cloud computing regulations, points out the gaps in modern Russian legislation in this sphere as well as the problems of legal protection for confidential data based on cloud solutions usage. The analysis of legal documents related to the personal data processing in the cloud.

Keywords: personal data, cloud computing, Amazon Web Services (AWS), cloud solutions for information security and data processing, confidential data, cross-border transfers of personal data from the EEA.

E.P. Afanasiev

DATA PROTECTION IN DOCUMENT-ORIENTED TECHNOLOGY APPLICATION (ON THE EXAMPLE OF "ELECTRONIC GOVERNMENT" SISTEM)

The purpose of this article is a review of theoretical and practical information security issues in document-oriented technology on the example of "electronic government".

In the present paper the author has identified the existing e-government problems, in particular, has examined weaknesses in the subsystem information security: risks and existing threats are analyzed, the information leakage channels are identified. The concept of existing decisions in the "electronic government" relating to information security (infrastructure, authentication, private key protection system) is defined. In addition, specific recommendations for data protection improving methods in the "electronic government" are given. The recommendations relate primarily to organizational practices.

Keywords: electronic document management, document-oriented technology, electronic government, information security subsystem.

G.A. Shevtsova

DEVELOPMENT OF FACTORY AUTOMATION SYSTEM AND INFORMATION SECURITY IN TERMS OF INFORMATION PROCESSING TECHNOLOGY

Information technology is inextricably linked with the information system, which is considered as the technological chain of message processing. Converting information into messages is processed using the character set encoding algorithms, and messages into information – using decoding of incoming character set. Information processing is considered as a conversion of one electronic data to other, differing from the original by information content, structure, form, and transformation result is a new kind of "order." The resulting electronic document is considered in conjunction with the electronic medium. Electronic document protection includes technology protection that is directly document processing chain protection.

Keywords: electronic document management, electronic data, information system protection, information technology, information coding and dissemination.

S.A. Zheltov

ADAPTATION FACTORIZATION PROBLEM SOLUTION BY SHERMAN–LEHMAN METHOD TO THE COMPUTING ARCHITECTURE CUDA

The article is devoted to some aspects of parallel computing and GPGPU technology used for solving the integer factorization. Major sections are devoted to the computing architecture CUDA review, its characteristics and Sherman–Lehman method adaptation to parallel computation on graphics hardware.

Keywords: parallel computation, integer factorization, CUDA architecture.

A.E. Baranovich

SEMANTIC ASPECTS OF INFORMATION SAFETY. CRYPTOSEMANTICS

In a context of the information-evolutionary approach to the system analysis and objective reality modeling, the basic aspects research of anthropomorphous information safety maintenance and anthropogenous various genesis systems are considered. The main attention in the present work is concentrated on the cryptosemantics – a new direction of intelligent systems information resources security protection from their not authorized use. As the general cryptology section, the cryptosemantics are characterized by a number of basic differences from classical cryptography and leans against own axiomatic basis. The article continues a cycle of works devoted to semantic-pragmatical aspects of information safety maintenance.

Keywords: information safety, intelligent systems, cryptology, cryptosemantics, semantics.

A.S. Zaytsev, A.A. Malyuk

INVESTIGATION OF INFORMATION SECURITY INTERNAL INTRUDER PROBLEM

This paper deals with the problem of information security internal intruder. The problem has been comprehensively examined and the existing internal intruder models have been considered. Relying on this analysis an imitation system dynamics model of internal intruder has been constructed. This model is supposed to give financial assesses. So an attempt to formalize the model using the technique of expert poll was made. Finally the further improvement of the model with expert role minimization was considered.

Keywords: internal intruder, system dynamics, imitation modeling, expert poll.

V.R. Grigoriev, A.P. Nikitin

STATIC METHODS FOR BIOMETRIC USER AUTHENTICATION

The PC's user's authentication task is considered by his keyboard writing. There is an approach which gives an opportunity to carry out the PC's user identification system by his traits of work with the PC. To solve the problem of PC's user's identification some statistical methods are suggested. This shows that the biggest efficiency for the PC's identification among the considered methods is reached by using Mann-Whitney's criterion.

Keywords: keyboard handwriting, user identification, biometrical authentication.

A.N. Korolev, A.A. Tarasov

ON THE FUNCTIONAL TOLERANCE OF NAVIGATION AND INFORMATION SYSTEMS

This article considers an approach to the description of the navigation and information systems structural organization in terms of their functional tolerance. Criteria, boundaries and stability of the functional navigation and information systems reserves are defined. The basic strategy for navigation and information systems reconfiguration with the destructive effects on them in order to provide automatic recovery of their health is specified.

Keywords: navigation and information system, functional stability, navigation field, destructive effect, functional reconfiguration.

S.V. Zapechnikov, A.S. Polyakova

INVESTIGATION OF OPTIMAL INFORMATION SECURITY INVESTMENT MODELS

Nowadays companies spend their financial resources irrationally: up to $^{2}/_{3}$ of funds are spent in vain. Lack of principles and recommendations for choosing optimal information security investment level requires the corresponding evaluating model development. This article presents the research of Gordon–Loeb model for evaluating the optimal information security investment level and the interdependent

risks model. One is provided by practical recommendations for choosing and applying models, for choosing the vulnerabilities range to concentrate financial resources on, models weak points are discussed.

Keywords: optimal information security investment, Gordon–Loeb model, interdependent security risks model.

A.E. Baranovich, D.B. Khankovsky

THINKING SUBPROCESSES INTERACTION MODELING ON LEVELS "CONSCIOUS–UNCONSCIOUS"

In the course of information-evolutionary approach to systems analysis and intelligent systems modeling, thinking subprocesses interaction mechanisms on levels of "conscious"–"unconscious" are investigated. The possibility of constructing a correspondence between the information objects models of thinking subprocesses with different etymology is shown. Thus the algorithmic implementation basis of the thinking subprocesses models interaction on various levels in the "artificial intelligence" anthropogenically-technical system is formed. The article continues series of papers devoted to the universal mechanisms modeling of various genesis intellectual activity.

Keywords: information, thinking, knowledge, intelligence system, consciousness, unconsciousness.

S.M. Iglitskaya

AN APPROACH TO POLYPHONIC MUSICAL TEXT SEMANTICS MODELING

The article is devoted to the musical text information component study. The possibility of using a universal model of complex dynamical systems states for polyphonic musical text semantics modeling is considered. Some conceptual approaches to the musical texts models construction for different styles are specified.

Keywords: musical text, text semantics, strict style polyphonic, k-hyperspace of SH-hypertopograph, SH-hyper-toponetworks.

A.N. Priezzhaya

PROTECTED INFORMATION SYSTEMS DESIGN

The process of developing an information system in a secure execution requires laborious protected object analysis and extensive documentation development. This paper describes a technique based on the models automated transformation, which allows to simultaneously develop multiple object representations, including threat and intruder models, and to build automatically on their base an information system model in a secure design.

Keywords: UML Model, automation, automated system development, transformation model, object model

A.S. Platonova

DATABASE DESIGN FOR EDUCATION RESULTS CONTROL AND EVALUATION INFORMATION SYSTEM

Article is devoted database design intended for ordered storage of the psychology-pedagogical information about education results control and evaluation: educational and control-measuring materials, student answers and teacher records and any other service information. Designing of information storage structure is carried out at levels of conceptual, logical and physical database design, the related models complex is constructed as a result.

Keywords: education results control and evaluation, psychology-pedagogical information storage, database, semantic model, datalogical model, MySQL, physical model.

A.A. Pupykina

GRAPH STRUCTURE OF RELATED MODULES WHILE DESIGNING USER INTERFACE MODEL OF LEARNING ENVIRONMENT

Based on the requirements for user interface designing methods of the learning environment,the article describes a learning environment model provided in the form of a related modules system, forming graph

structures. To design user interface adaptation tools the cognitive states maps are proposed.

Keywords: graph, cognitive states map, model, model-based approach, learning environment, user interface.

O.V. Kazarin

MODELS AND METHODS FOR PROACTIVE SOFTWARE PROTECTION

In this paper, we consider models and methods for proactive information system software defense, as the defense which is based on mechanisms taking into account its functional properties, architectural and technological features of the external system environment at all stages before program usage as intended. In particular, at the stage preceding the stages of program testing.

Keywords: proactive protection, software protection, software lifecycle.

A.N. Priezzhaya

GENERATION OF INFORMATION SYSTEM SECURITY THREATS MODEL

The threat model developing process requires time-consuming analysis of the protected object. This paper describes a technique based on the automated transformation of models, which allows to simultaneously develop multiple object representations, including text description and to build automatically on their base threats and intruder models.

Keywords: UML model, personal information, model transformation, threat model, object model.

Сведения об авторах

Афанасьев Евгений Павлович – аспирант кафедры компьютерной безопасности Института информационных наук и технологий безопасности при Российском государственном гуманитарном университете (ИИНиТБ РГГУ), afanasiev.ev@yandex.ru

Баранович Андрей Евгеньевич – доктор технических наук, профессор кафедры компьютерной безопасности ИИНиТБ РГГУ, barae@rambler.ru

Григорьев Виталий Робертович – кандидат технических наук, главный научный консультант ЗАО РНТ, grigorjev_vr@mail.ru

Желтов Сергей Александрович – старший преподаватель кафедры компьютерной безопасности и математических методов управления ТвГУ, zheltov_s@mail.ru

Зайцев Антон Сергеевич – студент Национального исследовательского ядерного университета МИФИ, Anthony.Zaytsev@gmail.com

Запечников Сергей Владимирович – доктор технических наук, доцент, Национальный исследовательский ядерный университет МИФИ, профессор кафедры «Информационная безопасность банковских систем», SVZapechnikov@mephi.ru

Иглицкая Софья Михайловна – аспирантка кафедры общей информатики ИИНиТБ РГГУ, sofa.sofa@mail.ru

Казарин Олег Викторович – доктор технических наук, ведущий научный сотрудник, отдел математических проблем информационной безопасности Института проблем информационной безопасности МГУ, okaz2005@yandex.ru

Королев Александр Николаевич – кандидат технических наук, старший научный сотрудник, начальник отдела ОАО «Российские космические системы», kan196374@yandex.ru

Ларин Дмитрий Александрович – кандидат технических наук, доцент кафедры ИТС МИРЭА, greattzar@yandex.ru

Малюк Анатолий Александрович – кандидат технических наук, профессор, Национальный исследовательский ядерный университет МИФИ, AAMalyuk@mephi.ru

Никитин Андрей Павлович – аспирант МГТУ МИРЭА, gouststalker@mail.ru

Платонова Алла Сергеевна – соискатель кафедры «Физика и прикладная математика» Муромского института (филиала) ФГБО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», allaplatonova@inbox.ru

Полякова Анна Сергеевна – Национальный исследовательский ядерный университет МИФИ, студентка кафедры «Информационная безопасность банковских систем», Anna.Polyakova.des@gmail.com

Приезжая Алина Николаевна – аспирант кафедры компьютерной безопасности ИИНиТБ РГГУ, priezzhaya@gmail.com

Пупыкина Анна Александровна – аспирантка ИИНиТБ РГГУ, anna.pupikina@gmail.com

Тарасов Александр Алексеевич – доктор технических наук, профессор, директор Института информационных наук и технологий безопасности РГГУ, aa_tarasov@list.ru

Ханковский Дмитрий Борисович – аспирант кафедры общей информатики ИИНиТБ РГГУ, http://samtcenter.ru/

Чемеркин Валерий Валерьевич – аспирант кафедры компьютерной безопасности ИИНиТБ РГГУ, yury.chemerkin@gmail.com

Шевцова Галина Александровна – кандидат исторических наук, доцент кафедры организационно-правовой защиты информации ИИНиТБ РГГУ, shevtsova-g@rambler.ru

General data about the authors

Afanasiev Eugeny – postgraduate student of computer security department in Institute for Information Sciences and Security Technologies of Russian State University for the Humanities (IISaST of RSUH), afanasiev.ev@yandex.ru

Baranovich Andrew – Ph.D. in Engineering, professor of computer security department in IISaST of RSUH, barae@rambler.ru

Grigoriev Vitaly – candidate of technical sciences, main scientific consultant of RNT cjsc, grigorjev_vr@mail.ru

Zheltov Sergey – Senior lecturer in computer security and control of mathematical methods TSU, zheltov_s@mail.ru

Zaytsev Anton – student, National Research Nuclear University "MEPhI", Anthony.Zaytsev@gmail.com

Zapechnikov Sergey – Ph.D. in Engineering, National Research Nuclear University "MEPhI", professor of Information Security of Banking Systems department, SVZapechnikov@mephi.ru

Iglitskaya Sofya – postgraduate student of computer science department of IISaST of RSUH, sofa.sofa@mail.ru

Kazarin Oleg – Ph.D. in Engineering, leading researcher, Department of Information Security Mathematical Problems in Information Security Issues Institute, Moscow State University, okaz2005@yandex.ru

Korolev Alexander – candidate of technical science, senior researcher, head of JSC "Russian space systems", kan196374@yandex.ru

Larin Dmitry – candidate of technical science, associate professor of ITS MIREA, greattzar@yandex.ru

Malyuk Anatoliy – PhD (Engineering), professor, National Research Nuclear University "MEPhI", AAMalyuk@mephi.ru

Nikitin Andrey – postgraduate student MSTU "MIREA", gouststalker@mail.ru

Platonova Alla – postgraduate student of Murom Institute (branch) Federal state budgetary educational institution of Higher Professional Education "Vladimir State University named after Alexander Grigoryevich and Nickolay Grigoryevich Stoletovs", allaplatonova@inbox.ru

Polyakova Anna – National Research Nuclear University "MEPhI", student of Information Security of Banking Systems department, Anna.Polyakova.des@gmail.com

Priezzhaya Alina – postgraduate student of computer security department in Institute for Information Sciences and Security Technologies of Russian State University for the Humanities (IISaST of RSUH), priezzhaya@gmail.com

Pupykina Anna – postgraduate in IISaST of RSUH, anna.pupikina@gmail.com

Tarasov Alexander – Ph.D. in Engineering, professor, director of Institute for Information Sciences and Security Technologies of Russian State University for the Humanities, aa_tarasov@list.ru

Khankovsky Dmitry – postgraduate in IISaST of RSUH, http://samtcenter.ru/

Chemerkin Yury – postgraduate of computer security department in IISaST of RSUH, yury.chemerkin@gmail.com

Shevtsova Galina – candidate of historical science, assistant professor of organizational and legal information protection department in IISaST of RSUH, shevtsova-g@rambler.ru

Заведующая редакцией *И.В. Лебедева*
Художник *В.В. Сурков*
Художник номера *В.Н. Хотеев*
Корректор *Н.П. Гаврикова*
Компьютерная верстка *Г.И. Гаврикова*

Формат 60×90 1/16.
Уч.-изд. л. 17,7. Усл. печ. л. 17,0.
Тираж 1050 экз. Заказ № 173.

Издательский центр
Российского государственного
гуманитарного университета
125993 Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru